File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
(c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD=200654
(c) 2006 The Thomson Corporation

Set	Items	Description
S1	13411	SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR SUBSTITUTION()(TABLE? ? OR MATRIX?? OR MATRICE? ?) OR LUT? ? OR (LOOKUP OR LOOK()UP)()TABLE? ?
S2	3051	S1(5N)(ESTABLISH? OR SET????()UP OR SETUP OR DERIV??? OR CALCULAT? OR COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR GENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC????? OR BUILT OR BUILD?)
S3	2601952	PROGRAM? ? OR APPLICATION? ? OR SOFTWARE OR CODE? ? OR ROUTINE? ? OR SUBROUTINE? ? OR SUBPROGRAM? ? OR INSTRUCTION? ? OR DLL? ? OR LINK()LIBRAR??? OR OBJECT? ?
S4	150457	(PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ?)(5W)S3
S5	483344	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR SECOND? OR 2ND OR REMAINING)(2W)(PART? ? OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? OR FRACTION? ? OR MODULE?)
S6	271581	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR SECOND??? OR 2ND OR REMAINING)(2W)(ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR PACKET? ? OR FRAME? ?)
S7	709	(REMAINDER OR REST)(3W)S3
S8	37796	ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9	1243	S8(10N)S4:S7
S10	5	S2 AND S9
S11	13	S1 AND S9
S12	13	S10:S11

12/2/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0013534641
WPI ACC NO: 2003-628145/200360
XRPX Acc No: N2003-499837
Swing type block code enciphering **method**
Patent Assignee: SOFTWARE INST CHINESE ACAD SCI (SOFT-N)
Inventor: FENG D; ZHANG Y
Basic Patent 2 patents, 1 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
CN 1426191	A	20030625	CN 2001140475	A	20011210	200360	B

Priority Applications (no., kind, date): CN 2001140475 A 20011210
CN A
NOVELTY - This invention relates to a grouped ciphering method including dividing clear text data into groups of clear text data, designing keying **forming** a **S box** (replacement list) made up of 256 elements; as the initial condition of shift register, the clear text data shift right a certain beats in first nonlinear logic then shift left a certain beats according to second nonlinear logic then repeats just like playing swing till the pre-designed turns to output the obtained shift register condition as the cipher set corresponding to the clear text set, and nonlinear logic relations between them is made up of feedback variations through **S box** many times. Condition changes of shift register cleverly enforce clear text mixture and divergence.

Title Terms/Index Terms/Additional Words: SWING; TYPE; BLOCK; CODE; ENCIPHER; METHOD

Class Codes
International Classification (Main): H04L-009/00

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-D01; W01-A05A

12/2/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0012810090 - Drawing available
WPI ACC NO: 2002-667222/200271
XRPX Acc No: N2002-527905
Establishing initial synchronization for link between mobile terminal and base station in cellular radio communication network in way that avoids deadlock conditions
Patent Assignee: INTERDIGITAL TECHNOLOGY CORP (INTE-N)
Inventor: ALPASLAN D; ALPASLAND D; DEMIR A; GRIECO D M; GRIECO D
Basic Patent 20 patents, 99 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2002069551	A1	20020906	WO 2002US3217	A	20020204	200271	B

Priority Applications (no., kind, date): US 2005205846 A 20050817; US 2002120735 A 20020411; US 200283796 A 20020227; US 2001271642 P 20010227; US 2001918611 A 20010731
National Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

Regional Designated States: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW AL LI LT LV MK RO SI BG CZ EE HU IS PL SK BA HR YU

Alerting Abstract WO A1

NOVELTY - Involves determining a chip offset of the strongest path detected over a frame of samples. In response to the determined chip offset, a scrambling code group number and slot offset are generated to retrieve the second synchronization code. A primary scrambling code is retrieved, in response to the code group number, to synchronize the user equipment to the base station.

DESCRIPTION - An INDEPENDENT CLAIM is included for a system.

USE - For establishing initial synchronization for the link between mobile terminal and a base station in a cellular radio communication network.

ADVANTAGE - Uses window exclusion logic in order to avoid a deadlock condition upon a detection of the wrong public land mobile network (PLMN).

DESCRIPTION OF DRAWINGS - The drawing shows a block diagram of the system used to implement the method.

Title Terms/Index Terms/Additional Words: ESTABLISH; INITIAL; SYNCHRONISATION; LINK; MOBILE; TERMINAL; BASE; STATION; CELLULAR; RADIO; COMMUNICATE; NETWORK; WAY; AVOID; DEADLOCK; CONDITION

Class Codes

International Classification (Main): G06F-017/30, H04B-001/18, H04B-001/707, H04B-007/26, H04J-013/00, H04L, H04L-007/04
(Additional/Secondary): H04B-017/00, H04B-007/00, H04L-007/02, H04Q-007/00, H04Q-007/20, H04Q-007/38, H04J-003/06, H04L-007/00
International Classification (+ Attributes)
IPC + Level Value Position Status Version
H04L-0007/02 A I F B 20060101
H04B-0001/707 A I R 20060101
H04B-0001/707 A I F B 20060101
H04Q-0007/38 A I L B 20060101
H04B-0001/707 C I R 20060101
US Classification, Issued: 370503000, 370441000, 370503000, 380274000, 370503000, 380274000, 375362000, 375362000, 375362000, 375360000

File Segment: EPI;
DWPI Class: W01; W02
Manual Codes (EPI/S-X): W01-A01; W01-A04B; W01-B05A1A; W02-C03C1A; W02-C05; W02-G03A1; W02-K02A

12/2/4 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

0010988013 - Drawing available
WPI ACC NO: 2001-612804/
XRPX Acc No: N2001-457516
Electronic mail system deletes mail address of user after forwarding mail to other party' s message box , whose compatibility level satisfying preset tolerance is judged by referring to registered user information
Patent Assignee: DANBONET SYSTEMS KK (DANB-N)
Inventor: OZAKI K
Basic Patent 1 patents, 1 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
JP 2001053787	A	20010223	JP 1999229529	A	19990813	200171 B

Priority Applications (no., kind, date): JP 1999229529 A 19990813

Alerting Abstract JP A

NOVELTY - Host computer (1) connected to terminal equipments (3-1 - 3-n), registers user information in memory, based on which compatibility of user sending mail is judged. User's compatibility level satisfying preset tolerance is judged to generate common message box. Mail is forwarded to **other party** after **enciphering** mail address. User's mail address is deleted after forwarding mail to other party' **s** message **box** .

DESCRIPTION - The compatibility of the user is judged based on program stored in the host computer. The level of compatibility is calculated and the common message box is generated only when the compatibility level of user satisfies predetermined tolerance limit.

USE - Electronic mail system with user's secrecy protection function.

ADVANTAGE - Secrecy of the user is maintained by deleting the user's mail address after transmitting mail to the other party' **s** message **box** . Transmitting and receiving compatibility is judged effectively by referring to information stored in memory of host computer.

DESCRIPTION OF DRAWINGS - The figure shows the explanatory drawing of electronic mail system (The drawing includes non-English language text).

1 Host computer

3-1 - 3-n Terminal equipments

Title Terms/Index Terms/Additional Words: ELECTRONIC; MAIL; SYSTEM; DELETE; ADDRESS; USER; AFTER; FORWARDING; MESSAGE; BOX; COMPATIBLE; LEVEL; SATISFY; PRESET; TOLERANCE; JUDGEMENT; REFER; REGISTER; INFORMATION

Class Codes
International Classification (Main): H04L-012/54
(Additional/Secondary): G06F-013/00, H04L-012/58, H04L-029/08

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-H07C1; W01-A06E1; W01-A06G2; W01-A06X

12/2/5 (Item 5 from file: 350)

0010955558 - Drawing available
WPI ACC NO: 2001-578661/
XRPX Acc No: N2001-430577

Encryption program used for electronic mail security, includes instructions for performing mixing of data segments, swapping and substitution iteratively for preset times using different sub-keys

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: COPPERSMITH D; GENNARO R; HALEVI S; JUTLA C S; MATYAS S M; PEYRAVIAN M; SAFFORD D R; ZUNIC N

Basic Patent 1 patents, 1 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 6243470	B1	20010605	US 199818707	A	19980204	200165 B

Priority Applications (no., kind, date): US 199818707 A 19980204

Alerting Abstract US B1

NOVELTY - The programs include instruction to receive input data with each data segments having bytes equal to block length of variable length block for ciphering. The input data segments is mixed using XOR operations and **substitution box** (**S** - **box**) look-up operation. The mixed segments are swapped and XOR of swapped segments and **S** - **box** look-up are performed to **produce** substituted bytes. The process is iterated for preset times using different sub-keys.

DESCRIPTION - The sub-keys are generated using the symmetric input key distinctly for every round of encryption. INDEPENDENT CLAIMS are also included for the following:

1.Encryption system;

2.Encryption method

USE - For encrypting input data using block cipher algorithm for secure storage of e.g. customer accounts in bank, credit company.
ADVANTAGE - The block cipher algorithm allows variation of block size, key size and number of encryption cycles and uses logical XOR operation which reduces time used for encrypting and decrypting data.
DESCRIPTION OF DRAWINGS - The figure shows the flowchart of encryption process.

Title Terms/Index Terms/Additional Words: ENCRYPTION; PROGRAM; ELECTRONIC; MAIL; SECURE; INSTRUCTION; PERFORMANCE; MIX; DATA; SEGMENT; SUBSTITUTE; ITERATIVE; PRESET; TIME; SUB; KEY

Class Codes
International Classification (Main): H04L-009/06
US Classification, Issued: 380259000, 380037000, 380029000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-D01; T01-H01C2; T01-H07C1; T01-H07C5E; T01-J05A1; T01-J05A2; T01-J12C; W01-A05A

12/2/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0010855984 - Drawing available
WPI ACC NO: 2001-474786/
XRPX Acc No: N2001-351382
Computer-readable code for providing a byte symmetric key block cipher, has computer-readable program code section used for treating substituted bytes as input data bytes for subsequent iteration
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: COPPERSMITH D; GENNARO R; HALEVI S; JUTLA C S; MATYAS S M; PEYRAVIAN M; SAFFORD D R; ZUNIC N
Basic Patent 1 patents, 1 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 6192129	B1	20010220	US 199818630	A	19980204	200151 B

Priority Applications (no., kind, date): US 199818630 A 19980204

Alerting Abstract US B1
NOVELTY - A byte value is determined by performing a third XOR operation followed by a second **S - box** lookup operation to **create** multiple substituted bytes. A computer-readable program code section is used for treating the substituted bytes as input data bytes for a subsequent iteration of the program code section.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1.a byte-oriented symmetric key block cipher providing system;

2.a byte-oriented symmetric key block cipher providing method.

USE - For providing a byte symmetric key block cipher for encryption and decryption in computer system.
ADVANTAGE - Improves encryption strength while enhancing encryption efficiency. Maximizes the number of environments in which solution can be used. Enables efficient and error-free decryption of encrypted data.
DESCRIPTION OF DRAWINGS - The figure shows the flowchart of a logic used for data block encryption.

Title Terms/Index Terms/Additional Words: COMPUTER; READ; CODE; BYTE; SYMMETRICAL; KEY; BLOCK; CIPHER; PROGRAM; SECTION; TREAT; SUBSTITUTE; INPUT; DATA; SUBSEQUENT; ITERATIVE

Class Codes
International Classification (Main): H04L-009/06
US Classification, Issued: 380259000, 380037000, 380029000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-D01; T01-S01C; T01-S03; W01-A05A; W01-A06B5A; W01-A06G3

12/2/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0010223104 - Drawing available
WPI ACC NO: 2000-534301/
XRPX Acc No: N2000-395259
Authorizing film holder to access remote look - up table **of film photo finishing data, matching** encrypted segments **of access** code
Patent Assignee: EASTMAN KODAK CO (EAST)
Inventor: CIPOLLA D; SMART D C
Basic Patent 3 patents, 27 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 1016926	A2	20000705	EP 1999204275	A	19991213	200049 B

Priority Applications (no., kind, date): US 1998221942 A 19981228
Regional Designated States: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Alerting Abstract EP A2
NOVELTY - Film is registered by docking (138) in input device and reading first segment of identifier marked on film, which includes one or both **segments** of access **code** . One **segment** of access **code** is **encryption** of **other segment** . User or holder of film can only access data stored in **look - up table** (12) if code value obtained by decrypting first segment , matches second segment.
DESCRIPTION - Film is registered by docking in input device and reading first segment of identifier marked on film. Identifier includes one or both **segments** of access **code** . One segment is **encryption** of other. User or holder of film can only access data stored in **look - up table** (12) if code value obtained by decrypting first segment , matches **second segment** . Key used to decrypt **encrypted** first **segment** of access **code** , is maintained and supplied by input or photo finishing unit (14), or by gatekeeper part of **look - up table** . Key is based on symmetric encryption-decryption algorithm or asymmetric encryption-decryption algorithm.
USE - To access film photo finishing data stored in remote **look - up table** for one-time use camera.
DESCRIPTION OF DRAWINGS - View of system including access coded film unit.
12 **Look - up table**
14 Photo finishing unit

Title Terms/Index Terms/Additional Words: FILM; HOLD; ACCESS; REMOTE; UP; TABLE; PHOTO; FINISH; DATA; MATCH; ENCRYPTION; SEGMENT; CODE
Class Codes
International Classification (Main): G03B-017/02, G03B-027/46, G03D-015/00
(Additional/Secondary): G03B-017/24, G03B-017/48, G03B-027/72, G06F-017/30
US Classification, Issued: 396006000, 396311000, 396429000, 396512000,

355040000, 713185000

File Segment: EngPI; EPI;
DWPI Class: S06; T01; P82; P84
Manual Codes (EPI/S-X): S06-B04A5; T01-J05B

12/2/8 (Item 8 from file: 350)

0010133625 - Drawing available
WPI ACC NO: 2000-441771/200038
XRPX Acc No: N2000-329715
Packet data communication controller used in network communication, includes pair of switches which feed packet data directly to controller and write unit according to its operation condition
Patent Assignee: I-DATA INT AS (IDAT-N)
Inventor: STEEN S; STEEN S R; STEENBERG K; VIDECRANTZ P
Basic Patent 4 patents, 86 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 2000030262	A2	20000525	WO 1999DK625	A	19991112	200038 B

Priority Applications (no., kind, date): DK 19981481 A 19981112; US 1998109743 P 19981124
National Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW
Regional Designated States: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW LI

Alerting Abstract WO A2

NOVELTY - A data read transmission control unit receives the input data from system bus of a host and transmits it to transmission controller directly or through a compression and encryption unit according to the operation mode of a first switch. Similarly the receiving control unit directly transfers the received data to write unit or through decryption units, based on operation mode of second switch.

DESCRIPTION - When the first switch is in second mode, the received input data is fed to a data compression unit which compresses part of input data. The compressed data is contained in the **second section** of the data communication packet. A data **encryption** unit receives the packet through an integrity check value (ICV) calculation unit calculates ICV by numerically summing the data part of the packet. The calculated ICV is added to the end of the data packet, which is then encrypted by the encryption unit, based on transmission encryption key transferred from session key **look up table** (**LUT**). Then, the encrypted packet is transmitted to the network by network transmission controller, according to determined transmission data. The received data is directly fed to controller, when first switch is in first state. A data receiving control unit receives the data from network and feeds the data to the data decompression unit, when the second switch is in second state. The decryption unit decompresses the encrypted and compressed section of the received data packet. The decrypted data packet is fed to a decompression unit through ICV verification unit. The ICV verification unit calculates the ICV and compares it with value stored in packet. If any error is found, the packet is discarded and message is transmitted to the host system. If the values are identical, the data packet is fed to the decompression unit. Then, the data packet is supplied to the data write unit after decompression. An INDEPENDENT CLAIM is also included for method for processing data packet.

USE - For network communication e.g. for local area network (LAN), wide area network (WAN).

ADVANTAGE - By incorporating several functions in single electronic circuit, the time delay from one unit to next is considerably reduced compared to time delay between discrete electronic components. The network controller further more controls the transmission FIFO so as to guarantee the continuous supply of bytes from the transmission FIFO to the network transmission controller, this ensures that the transmission is extraordinarily fast. By continuously monitoring if the data communication packets processed one within the packet specifications of the network, any redundant operations are eliminated, and thus the number of data communication packet transmitted on the network is reduced. The ICV calculation and verification ensures that no excessive time is spent on corrupted data communication packets at the receiving end of the transmission, therefore the implementation of this calculation verification reduces unnecessary data communication packet processing. The switches ensures fast recognition of clear text and consequently bypassing or disabling the series configuration, respectively.

DESCRIPTION OF DRAWINGS - The figure shows the schematic block diagram explaining data encryption and decryption in communication controller.

Title Terms/Index Terms/Additional Words: PACKET; DATA; COMMUNICATE; CONTROL; NETWORK; PAIR; SWITCH; FEED; WRITING; UNIT; ACCORD; OPERATE; CONDITION

Class Codes
International Classification (Main): H03M-007/30, H03M-007/38
(Additional/Secondary): H04L-009/12
US Classification, Issued: 380255000, 380256000, 380257000, 380269000, 713168000

File Segment: EPI;
DWPI Class: U21; W01
Manual Codes (EPI/S-X): U21-A05A2; W01-A03B; W01-A05A; W01-A06B5A; W01-A06B5B; W01-A06G2

12/2/9 (Item 9 from file: 350)

0010094892 - Drawing available
WPI ACC NO: 2000-401721/200035
XRPX Acc No: N2000-300861
Encryption/decryption unit for encrypting plain text into cipher text with compatibility with all types of previous encryptors/decryptors
Patent Assignee: TOSHIBA IT SOLUTION KK (TOSH-N); TOSHIBA KK (TOKE)
Inventor: KAWAMURA S; SANO F; SHIMIZU H
Basic Patent 7 patents, 27 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 1005191	A1	20000531	EP 1999306989	A	19990902	200035 B

Priority Applications (no., kind, date): JP 2004368168 A 20041220; EP 1999306989 A 19990902; JP 1998337108 A 19981127
Regional Designated States: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Alerting Abstract EP A1

NOVELTY - Includes encryption/decryptor (11) for performing an encryption or decryption process. A substitutor (12) performs data substitution of an output from the encryption/decryptor to a set permutation table. A second encryption/decryptor (13) for performing an encryption or decryption process for an output from the first substitutor. A second substitutor (14) performs data substitution of an output from the second encryption/decryptor to a set permutation table. Finally a third encryption/decryptor (15) for performing an encryption or decryption

process for an output from the second substitutor. All encryption/decryption use the same algorithm.
USE - For encrypting plain text into cipher text.
ADVANTAGE - Implements single algorithm which is compatible with all the DES, triple-DES and DES-SS.
DESCRIPTION OF DRAWINGS - The drawing shows a schematic diagram of the encryption/decryption unit.
11 Encryption/decryptor
12 Substitutor
13 Second encryption/decryptor
14 Second substitutor
15 Third encryption/decryptor

Title Terms/Index Terms/Additional Words: ENCRYPTION; DECRYPTER; UNIT; PLAIN; TEXT; CIPHER; COMPATIBLE; TYPE

Class Codes
International Classification (Main): G09C-001/00, H04K-001/00, H04L-009/06
International Classification (+ Attributes)
IPC + Level Value Position Status Version
H04L-0009/06 A I F B 20060101
US Classification, Issued: 380028000, 380042000, 713191000

File Segment: EngPI; EPI;
DWPI Class: W01; P85
Manual Codes (EPI/S-X): W01-A05A

12/2/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0009322938
WPI ACC NO: 1999-254491/199921
Related WPI Acc No: 2001-482049; 2001-512821; 2002-061520
XRPX Acc No: N1999-189449
N-bit block of data encrypting
Patent Assignee: LUYSTER F C (LUYS-I)
Inventor: LUYSTER F C
Basic Patent 11 patents, 79 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 1999014889	A1	19990325	WO 1998US19255	A	19980916	199921	B

Priority Applications (no., kind, date): US 20013503 A 20011023; US 2000725596 A 20001129; US 2000506285 A 20000217; WO 1998US19255 A 19980916; US 199898905 P 19980902; US 199896921 P 19980818; US 199896788 P 19980817; US 199894632 P 19980730; US 199764331 P 19971030; US 199762992 P 19971023; US 199759142 P 19970917; US 1998154391 A 19980916
National Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW
Regional Designated States: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW LI

Alerting Abstract WO A1
NOVELTY - The method involves first bit-moving variable bits of a round segment of data derived from one of the first and second round segments of data by set numbers of bits where most of the resulting bits affect the n-bit block of data. The first bit-moving is an operation selected from a group consisting of circular bit-rotation by nonzero numbers of bits, logical bit-shift by nonzero numbers of bits, nonidentity bit-permutation.
DESCRIPTION - To compute the primary round segments (R0,R1) in the second

half round, the following procedure is used. First, linearly combine (block (130) using the operator (L4) the primary segment (R0) with the sub-key K3) to produce an intermediate round segment. Linearly combine (block (132) using the operator L5) that intermediate segment and Ri producing a replacement value of Ri. Then, extract (block (134) a value V from R0) by taking f of the lsb bits of register (R0). Rotate (block (136) the replacement value of RI by the value V just extracted. This resulting value of R1 after the rotation is the new value of Ri (block (138). Then rotate (block (140) the value of R0) rightward by f bits. The resulting value of (R0) is the new value of (R0).

An INDEPENDENT CLAIM is included for:

1.a binary block cipher data transformation system

2.a method of key expansion for block ciphers

USE - The invention relates to block cipher secret-key cryptographic systems and methods.

ADVANTAGE - The invention provides improvements in a secret-key cryptographic system and method which uses data-dependent rotations. The cryptographic systems and methods are secure using data-dependent rotation with a novel iterative calculation which is robust and may resists attacks by sophisticated algorithms which detect and take advantage of weak sub-keys to determine the keys of the cryptographic system. A novel mechanism and method provides quick key expansion, particularly for data-dependent encryption, which decreases the time required to prepare a block cipher to encrypt or decrypt digital packets of bytes. The cryptographic system and method use minimal numbers of **s - boxes** with a novel iterative **calculation** where the block cipher does not require an excessive startup time, yet is simple, secure and efficient for bulk encryption while uses no more on-chip cache than necessary. The invention provides a novel mechanism and method for complex key expansion, which uses a minimum amount of time to prepare a block cipher to encrypt or decrypt a large file and which nevertheless ensures that the sub-keys generated by the method reflect every bit of the key in a complex uncorrelated manner.

DESCRIPTION OF DRAWINGS - The drawing is an algorithmic flowchart of encryption method.

134 block
R0,R1 primary round segments
K3 sub-key
134 block
140 block
138 block
L4 operator
L5 operator
R0 register

Title Terms/Index Terms/Additional Words: N; BIT; BLOCK; DATA

Class Codes

International Classification (Main): G06F-001/24, G06F-001/26, H04K-001/04, H04L-009/28, H04L-009/606

US Classification, Issued: 380037000, 380028000, 380029000, 380037000, 713168000, 713171000, 713200000, 713201000, 380028000, 380044000, 713168000, 713171000, 713200000, 713201000, 380028000, 380044000, 713200000, 713201000, 380037000, 380255000, 380037000, 380028000, 380042000

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A05A

12/2/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0008265028 - Drawing available
WPI ACC NO: 1997-373140/
XRPX Acc No: N1997-309821
Inter-round mixing in iterated block substitution systems - using trickle and quick trickle permutations for inter round permutations of sub blocks or individual bits to obtain respectively row completeness or quasi row completeness in Latin squares
Patent Assignee: TELEDYNE ELECTRONIC TECHNOLOGIES (TDCO); TELEDYNE IND INC (TDCO)
Inventor: MITTENTHAL L
Basic Patent 6 patents, 73 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 1997025799	A1	19970717	WO 1997US367	A	19970103	199734 B

Priority Applications (no., kind, date): US 1997888884 A 19970707; US 1997888454 A 19970707; US 1996584523 A 19960111
National Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN
Regional Designated States: AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

Alerting Abstract WO A1
The method of **encryption** involves receiving **successive blocks** of data, each being sub-divided into sub-blocks of data. Each sub-block is assigned to one of the individual **substitution boxes** . A statistically optimised permutation is selected.
It is determined if a set of preselected exponents is to be applied to the permutation. The set of preselected exponents is applied to the permutation if it is determined that a set of preselected exponents is to be applied, otherwise an exponent of one to the permutation is applied. After each round of encryption, an output of each numbered **substitution box** is applied as an input to the **substitution box** whose number is indicated by the permutation. The last two stages are repeated for a predetermined number of rounds.
USE/ADVANTAGE - Iterated block substitution system in which block **substitution tables** and pattern of inter round mixing are changed frequently. Interactions between sub blocks enhance mixing process and allow for inter round mixing in which sub blocks rather than individual blocks are permuted.

Title Terms/Index Terms/Additional Words: INTER; ROUND; MIX; BLOCK; SUBSTITUTE; SYSTEM; TRICKLE; QUICK; PERMUTATION; SUB; INDIVIDUAL; BIT; OBTAIN; RESPECTIVE; ROW; COMPLETE; QUASI; LATIN; SQUARE

Class Codes
International Classification (Main): H04L-009/00, H04L-009/06, H04L-009/28
US Classification, Issued: 380028000, 380029000, 380037000, 380042000, 380028000, 380037000, 380042000, 380028000, 380037000, 380042000

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A05

12/2/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0008214534 - Drawing available
WPI ACC NO: 1997-319373/199729
Related WPI Acc No: 1998-008265

XRPX Acc No: N1997-264424
Dynamic packet headers and multiple levels of packet encryption - using password authentication and s^3 DES to encrypt different portions **of logon packet with different keys based on nature of communication link**
Patent Assignee: NGUYEN M C (NGUY-I)
Inventor: NGUYEN M C
Basic Patent 1 patents, 1 countries

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 5638448	A	19970610	US 1995547346	A	19951024	199729 B
			US 1996583933	A	19960111	

Priority Applications (no., kind, date): US 1995547346 A 19951024; US 1996583933 A 19960111

Alerting Abstract US A
The method of securely transmitting packet data between a client and a server with packets encrypted by **S - box** data involves using at least one communication channel to transmit packets between at least one client and a server. A first logon packet including information identifying the client source system is encrypted in the client and transmitted to the server. The logon packet is decrypted in the server.
A **second** logon **packet** is **encrypted** in the server with client authenticating information and transmitted to the client. The second logon packet is decrypted in the client. A third logon packet with session information is encrypted in the client and transmitted to the server. The third logon packet is then decrypted in the server. A fourth logon packet is encrypted in the server with session information and transmitted to the client. The fourth logon packet is decrypted in the client. Encrypted data packets are transmitted between the client and server which are encrypted using **S - box** encryption. The client and server can establish secure communications by bi-directionally transmitting encrypted data.
USE/ADVANTAGE - Ensures that access to data is restricted to authorised parties whilst providing consistent performance.

Title Terms/Index Terms/Additional Words: DYNAMIC; PACKET; HEADER; MULTIPLE ; LEVEL; ENCRYPTION; PASSWORD; AUTHENTICITY; DES; PORTION; KEY; BASED; NATURE; COMMUNICATE; LINK

Class Codes
International Classification (Main): H04L-009/06
(Additional/Secondary): H04L-009/00, H04L-009/32
US Classification, Issued: 380029000, 380009000, 380021000, 380023000, 380025000, 380037000, 380043000, 380049000

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A03B; W01-A05B; W01-A06F; W01-A06G2

12/2/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0007285501
WPI ACC NO: 1995-344810/199544
Related WPI Acc No: 1995-131556
XRPX Acc No: N1995-257690
Encryption and decryption look up table generator **- generates tables in accordance with session key and temporarily stores them in memory to convert message to code**
Patent Assignee: CHANTILLEY CO LTD (CHAN-N); CHANTILLEY CORP LTD (CHAN-N)
Inventor: HAWTHORNE W; HAWTHORNE W M
Basic Patent 7 patents, 62 countries

Patent	Application

Number	Kind	Date	Number	Kind	Date	Update
WO 1995026087	A1	19950928	WO 1995GB660	A	19950323	199544 B

Priority Applications (no., kind, date): GB 19945766 A 19940323
National Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NL NO NZ PL PT RO RU SD SE SG SI SK TJ TT UA US UZ VN
Regional Designated States: AT BE CH DE DK ES FR GB GR IE IT KE LU MC MW NL OA PT SD SE SZ UG

Alerting Abstract WO A1

The encryption/decryption device enables encrypted communication between two stations, each incorporating such an appts. The appts. is arranged to **generate** a set of **look - up tables** in accordance with a session key and temporarily stores the tables in memory. Each successive element of a message is converted to a code through use of the **look - up tables** .

Pref., the device is arranged for use of a fresh session key at intervals during the course of each transmission. Each element of the message is converted to its code by a procedure which involves addressing one of the **look - up tables** and using the output of that table to address another of the **look - up tables** .

USE/ADVANTAGE - Telephone, computer and facsimile data encryption system. Fast generation of tables and therefore procedure.

Title Terms/Index Terms/Additional Words: ENCRYPTION; DECRYPTER; UP; TABLE; GENERATOR; GENERATE; ACCORD; SESSION; KEY; TEMPORARY; STORAGE; MEMORY; CONVERT; MESSAGE; CODE

Class Codes
International Classification (Main): H04L-009/06, H04L-009/08
(Additional/Secondary): G09C-001/00, H04L-009/00, H04N-001/44
US Classification, Issued: 380021000, 380009000, 380044000, 380046000, 380049000, 380050000

```
File   8:Ei Compendex(R) 1970-2006/Aug W2
         (c) 2006 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2006/Jun
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Aug 25
         (c) 2006 BLDSC all rts. reserv.
File   2:INSPEC 1898-2006/Aug W2
         (c) 2006 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2006/May W2
         (c)2006 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2006/Aug W2
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Jul W5
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 2006 The Thomson Corp
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Aug W3
         (c) 2006 The Thomson Corp
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Jul
         (c) 2006 The HW Wilson Co.
File 266:FEDRIP 2005/Dec
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2006/Aug W3
         (c) 2006 FIZ TECHNIK
File  62:SPIN(R) 1975-2006/Apr W4
         (c) 2006 American Institute of Physics
File 239:Mathsci 1940-2006/Oct
         (c) 2006 American Mathematical Society

Set     Items   Description
S1      22063   SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR
              SUBSTITUTION()(TABLE? ? OR MATRIX?? OR MATRICE? ?) OR LUT? ?
              OR (LOOKUP OR LOOK()UP)()TABLE? ?
S2       3314   S1(5N)(ESTABLISH? OR SET????()UP OR SETUP OR DERIV??? OR C-
              ALCULAT? OR COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR G-
              ENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR F-
              ORMING OR FORMATION? ? OR PRODUC????? OR BUILT OR BUILD?)
S3   10916783   PROGRAM? ? OR APPLICATION? ? OR SOFTWARE OR CODE? ? OR ROU-
              TINE? ? OR SUBROUTINE? ? OR SUBPROGRAM? ? OR INSTRUCTION? ? OR
              DLL? ? OR LINK()LIBRAR??? OR OBJECT? ?
S4     299559   (PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? -
              OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEM-
              ENT? ? OR ZONE? ? OR REGION? ?)(5W)S3
S5     394041   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR S-
              UBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT -
              OR SECOND? OR 2ND OR REMAINING)(2W)(PART? ? OR PORTION? ? OR -
              FRAGMENT? ? OR SECTION? ? OR SEGMENT? OR FRACTION? ? OR MODUL-
              E?)
S6     357880   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR S-
              UBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT -
              OR SECOND??? OR 2ND OR REMAINING)(2W)(ASPECT? ? OR BLOCK? ? OR
              ELEMENT? ? OR ZONE? ? OR REGION? ? OR PACKET? ? OR FRAME? ?)
S7       1350   (REMAINDER OR REST)(3W)S3
S8      49458   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9        276   S8(10N)S4:S7
S10         0   S2 AND S9
S11         4   S1 AND S9
S12         4   RD  (unique items)
```

12/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04068920 E.I. No: EIP95022558427
Title: On the security of the CAST encryption algorithm
Author: Heys, H.M.; Tavares, S.E.
Corporate Source: Queen's Univ, Kingston, Ont, Can
Conference Title: Proceedings of the 1994 Canadian Conference on Electrical and Computer Engineering. Part 1 (of 2)
Conference Location: Halifax, Can Conference Date: 19940925-19940928
Sponsor: Canadian Society for Electrical and Computer Engineering; IEEE
E.I. Conference No.: 42396
Source: Canadian Conference on Electrical and Computer Engineering v 1 1994. IEEE, Piscataway, NJ, USA. p 332-335
Publication Year: 1994
CODEN: 001780
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9504W3
Abstract: In this paper we examine a new private key encryption algorithm referred to as CAST. Specifically, we investigate the security of the cipher with respect to linear cryptanalysis. From our analysis we conclude that it is easy to select **S - boxes** so that an efficient implementation of the CAST algorithm is demonstrably resistant to linear cryptanalysis. (Author abstract) 9 Refs.
Descriptors: *Algorithms; Security of data; Computer software; Logic gates; Iterative methods; Function evaluation; Approximation theory; Probability
Identifiers: CAST **encryption** algorithm; Round function; Linear cryptanalysis; Private key **block** ciphers; **Software** implementation; Data **encryption** standard
Classification Codes:
723.1 (Computer Programming); 723.2 (Data Processing); 721.3 (Computer Circuits); 921.6 (Numerical Methods)
723 (Computer Software); 721 (Computer Circuits & Logic Elements); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

12/5/2 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01691684 ORDER NO: AADMQ-36013
SECURITY ASPECTS OF SUBSTITUTION-PERMUTATION ENCRYPTION NETWORKS
Author: CHEN, ZHI-GUO
Degree: M.SC.
Year: 1998
Corporate Source/Institution: QUEEN'S UNIVERSITY AT KINGSTON (CANADA) (0283)
Adviser: STAFFORD TANARES
Source: VOLUME 37/04 of MASTERS ABSTRACTS.
PAGE 1241. 104 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL ; COMPUTER SCIENCE
Descriptor Codes: 0544; 0984
ISBN: 0-612-36013-X

This thesis investigates some security aspects of basic substitution-permutation **encryption** networks (SPNs). Compared to **other block** ciphers, SPNs have many desirable and predictable cryptographic properties which are very useful for the design and analysis of cryptosystems.
We start with an estimate and upper bound on the nonlinearity

distribution of **s - boxes** which shows that low nonlinearities are very unlikely for large **s - boxes** . This further confirms the statement that large **s - boxes** have better cryptographic properties. In addition, we use statistical methods to measure the distance between SPNs and the ideal cipher. Based on the experimental results on XOR table distributions and supported by the results on nonlinearity, we show that SPNs converge to the ideal cipher with an increasing number of rounds. We also present a new differential-like attack which is easy to implement and outperforms the classical differential crypt-analysis on the basic SPN structure. In particular, it is shown that 64-bit SPNs with 8 x 8 **s - boxes** are resistant to our attack after 12 rounds. From the attack, it can be seen that the number of active **s - boxes** is very important. For a secure SPN, it is necessary to make the number of active **s - boxes** in the last round independent of the number of active **s - boxes** in previous rounds. In this respect, it is found that the number of active **s - boxes** in the last round becomes independent of the number of active **s - boxes** in the first round for basic SPNs with an increasing number of rounds. These experiments and the analytical results may be regarded as some evidence towards provable security for SPN cryptosystems.

12/5/3 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

16007795 PASCAL No.: 03-0153163
Differential and linear probabilities of a block-encryption cipher
JAKIMOSKI G; KOCAREV L
Institute for Nonlinear Science Univ. of California at San Diego, San Diego, CA 92093-0402, United States
Journal: IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2003, 50 (1) 121-123
ISSN: 1057-7122 CODEN: ITCAEX Availability: INIST-222 E81
No. of Refs.: 16 Refs.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: United States
Language: English
The differential and linear probabilities of a block-encryption cipher were discussed. It was assumed that that there was a three-round trail that possessed less than two active **S - boxes** . It was found that the algorithm proposed by the Jakimoski and Kocarev was secure against differential and linear attacks.

English Descriptors: **Block - encryption** cipher; Theory; **Codes** (symbols) ; Security of data; Algorithms; Probability; Cryptography; Experiments
French Descriptors: Theorie; Code(symbole); Securite donnee; Algorithme; Probabilite; Cryptographie; Experience

Classification Codes: 001D04B; 001D02B; 001D02B07B; 001A02; 001A02H01

12/5/4 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci

03781620 MR 2006b#94040
Affine equivalences in the AES round function.
Youssef, A. M. (Institute for Informatoin Systems Engineering, Sir George Williams Campus, Montreal, Quebec, H3G 1T7, Canada)
Tavares, S. E. (Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, K7L 3N6, Canada)
Corporate Source Codes: 3-CONC-ICE; 3-QEN-CP
Discrete Appl. Math.
Discrete Applied Mathematics. Combinatorial Algorithms, Optimization and

Computer Science, 2005, 148, no. 2, 161--170. ISSN: 0166-218X
CODEN: DAMADU
Language: English Summary Language: English
Document Type: Journal
Journal Announcement: 200511
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: SHORT (4 lines)
It is shown that all of the outputs of the advanced encryption standard (AES) round function are in the same affine equivalence class. It is not clear whether this fact could help in a cryptanalytic attack on AES.
Reviewer: Cusick, Thomas W. (1-SUNYB)
Review Type: Signed review
Descriptors: *94A60 -Information and communication, circuits-Communication, information-Cryptography (See also 11T71, 14G50, 68P25)

File 348:EUROPEAN PATENTS 1978-2006/ 200634
(c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060824UT=20060817
(c)

Set	Items	Description
S1	44886	SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR SUBSTITUTION()(TABLE? ? OR MATRIX?? OR MATRICE? ?) OR LUT? ? OR (LOOKUP OR LOOK()UP)()TABLE? ?
S2	10400	S1(5N)(ESTABLISH? OR SET????()UP OR SETUP OR DERIV??? OR CALCULAT? OR COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR GENERAT? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC????? OR BUILT OR BUILD?)
S3	2919835	PROGRAM? ? OR APPLICATION? ? OR SOFTWARE OR CODE? ? OR ROUTINE? ? OR SUBROUTINE? ? OR SUBPROGRAM? ? OR INSTRUCTION? ? OR DLL? ? OR LINK()LIBRAR??? OR OBJECT? ?
S4	248443	(PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ?)(5W)S3
S5	504813	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR SECOND? OR 2ND OR REMAINING)(2W)(PART? ? OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? OR FRACTION? ? OR MODULE?)
S6	673649	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR SECOND??? OR 2ND OR REMAINING)(2W)(ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR PACKET? ? OR FRAME? ?)
S7	3995	(REMAINDER OR REST)(3W)S3
S8	47144	ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9	4375	S8(10N)S4:S7
S10	11	S2(100N)S9
S11	49	S1(50N)S9
S12	53	S10:S11
S13	35	S12 AND AC=US/PR AND AY=(1978:2000)/PR
S14	35	S12 AND AC=US AND AY=1978:2000
S15	35	S12 AND AC=US AND AY=(1978:2000)/PR
S16	32	S12 AND PY=1978:2000
S17	38	S13:S16
S18	38	IDPAT (sorted in duplicate/non-duplicate order)

18/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01951853
Secure processor with external memory using block chaining and block re-ordering
Gesicherter Prozessor mit externem Speicher unter Verwendung von Block-Chaining und Wiederherstellung der Blockenreihenfolge
Processeur securise avec memoire externe utilisant le chainage par blocs et resequencement des blocs
PATENT ASSIGNEE:
GENERAL INSTRUMENT CORPORATION, (1403172), 101 Tournament Drive Horsham, , Pennsylvania 19044, (US), (Applicant designated States: all)
INVENTOR:
Candelore, Brant, 10124 Quail Glen Way, Escondido, California 92029, (US)
Sprunk, Eric, 6421 Cayenne Lane, Carlsbad, California 92009, (US)
LEGAL REPRESENTATIVE:
Hoeger, Stellrecht & Partner Patentanwalte (100381), Uhlandstrasse 14 c, 70182 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1571523 A1 050907 (Basic)
APPLICATION (CC, No, Date): EP 2005011051 981006;
PRIORITY (CC, No, Date): US 949111 971010
DESIGNATED STATES: DE; FR; GB; NL
RELATED PARENT NUMBER(S) - PN (AN):
EP 908810 (EP 98118843)
INTERNATIONAL PATENT CLASS (V7): G06F-001/00; G06F-012/14; H04L-009/32; H04L-029/06
ABSTRACT WORD COUNT: 147
NOTE:
Figure number on first page: 6

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200536	1997
SPEC A	(English)	200536	17196
Total word count - document A			19193
Total word count - document B			0
Total word count - documents A + B			19193

...SPECIFICATION machine code, or pseudo code or interpreted code, such as Java(TM). It may include **look - up tables** , stored keys, and various temporary data such as intermediate calculations and the state of the...

...It may even include some or all of the initialization vectors and keys used to **encrypt** /decrypt or verify/authenticate the **rest** of the **program** information in block chains. This can allow the same vector or key information to be...would actually be data which is never processed. The external storage device 110 may be **encrypted** such that the **blocks** of **program** information, and authentication information are stored in non-sequential address location in the storage device. It would be preferable to include the high order address bits in **encryption** of the storage device so that any **block** of **program** information may be located anywhere in the memory space. **Substitution tables** (S-tables) can be used to eliminate regularity and add non-linearity in the address ...

18/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00450088
ENCRYPTION METHOD

VERSCHLUSSELUNGSMETHODE
METHODE DE CHIFFREMENT
PATENT ASSIGNEE:
CRYPTECH, INC., (1343120), 34, Severn Parkway, Jamestown, NY 14701, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
WOOD, Michael, C., 147 Prather Avenue, Jamestown, NY 14701, (US)
LEGAL REPRESENTATIVE:
Land, Addick Adrianus Gosling et al (59332), Arnold & Siedsma, Advocaten en Octrooigemachtigden, Sweelinckplein 1, 2517 GK Den Haag, (NL)
PATENT (CC, No, Kind, Date): EP 489742 A1 920617 (Basic)
EP 489742 A1 930317
EP 489742 B1 971119
WO 9103113 910307
APPLICATION (CC, No, Date): EP 90911008 900314; WO 90US1391 900314
PRIORITY (CC, No, Date): US 395448 890817
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04L-009/06;
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9711W2	1540
CLAIMS B	(German)	9711W2	1499
CLAIMS B	(French)	9711W2	1646
SPEC B	(English)	9711W2	14641
Total word count - document A			0
Total word count - document B			19326
Total word count - documents A + B			19326

...SPECIFICATION the cryptographic system of the present invention. If there is more plaintext left to be **encrypted** , as determined by query 18, the **next block** of plaintext is selected at reference 20 and the **next block** is **encrypted** . If there is no more plaintext, then the system stops operation at reference 22.
The...

...tables in memory is shown in more detail in FIG. 2. A permutation table, an **S - box** table and an enclave table are initially loaded into the system's memory at reference...

18/3,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01165525
Method of secure database access for the holder of an image capture package
Verfahren zur Datenbank-Zugangssicherung fur den Benutzer einer Bildaufnahmeeinheit
Procede pour controler l'acces a une base de donnees pour l'utilisateur d'un systeme de capture d'images
PATENT ASSIGNEE:
EASTMAN KODAK COMPANY, (201212), 343 State Street, Rochester, New York 14650, (US), (Applicant designated States: all)
INVENTOR:
Smart, David C., Eastman Kodak Company, 343 State Street, Rochester, New York 14650-2201, (US)
Cipolla, David, Eastman Kodak Company, 343 State Street, Rochester, New York 14650-2201, (US)
LEGAL REPRESENTATIVE:
Weber, Etienne Nicolas et al (91684), Kodak Industrie, Departement Brevets, CRT, Zone Industrielle, 71102 Chalon sur Saone Cedex, (FR)
PATENT (CC, No, Kind, Date): EP 1016926 A2 000705 (Basic)

EP 1016926 A3 040204
APPLICATION (CC, No, Date): EP 99204275 991213;
PRIORITY (CC, No, Date): US 221942 981228
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G03D-015/00; G06F-017/30; G06F-012/14; H04N-001/44; H04N-001/21; H04N-001/327
ABSTRACT WORD COUNT: 75
NOTE:
Figure number on first page: 20A 20B

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200027	316
SPEC A	(English)	200027	15316
Total word count - document A			15632
Total word count - document B			0
Total word count - documents A + B			15632

...SPECIFICATION other holder of the film unit 10 access to the remotely stored data in the **look - up table** 12 if a code value obtained by decrypting a submitted first segment, matches a second segment. In accessing the **look - up table** 12, the film unit 10 is registered and the **encrypted** first **segment** of the access **code** 128 is detected. The registering preferably includes docking (138) the film unit 10 in an...

...ordinary alphanumeric characters.
In particular embodiments, the key 152 that is used to decrypt the **encrypted** first **segment** of the access **code** 128 is not recorded on the film unit 10. Referring to Figure 11, the key...

...152 can alternatively be maintained and supplied by a gatekeeper 130, a portion of the **look - up table** 12 that controls access to the logical memory units 20. The decryption can be performed...

...which could cause the corruption of valid information in logical memory units 20 in the **look - up table** 12. The key 152 can also take the form of a codebook, a table linking...

...now to Figures 14-15, in some embodiments, the film unit 10 bears only the **encrypted** first segment. The **second segment** is present only in the **look - up table** 12. The film unit 10 can include a serial number or label number that is...

...CLAIMS 10 wherein said decrypting further comprises maintaining a decryption key or code book in said **look - up table** .
12. The method of claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11 wherein said decrypting further comprises utilizing a symmetric or asymmetric **encryption** -decryption algorithm or a codebook of said first and **second segments** .

18/3,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01125455
CRYPTOGRAPHIC COMMUNICATION PROCESS AND APPARATUS
KRYPTOGRAPHISCHES VERMITTLUNGSVERFAHREN UND GERAT
PROCESSUS ET APPAREIL DE COMMUNICATION CRYPTOGRAPHIQUE
PATENT ASSIGNEE:
Tecsec, Incorporated, (1733051), 1953 Gallows Road, Suite 220, Vienna, VA 22182, (US), (Proprietor designated states: all)
INVENTOR:

SCHEIDT, Edward, M., 1048 Dead Run Drive, McLean, VA 22101, (US)
WACK, C., Jay, 13715 Lewisdale Road, Clarksburg, MD 20871, (US)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1260052 A2 021127 (Basic)
EP 1260052 B1 051019
WO 2000002340 000113
APPLICATION (CC, No, Date): EP 98933010 980702; WO 98US13626 980702
PRIORITY (CC, No, Date): US 108312 980701
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/00
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200542	1951
CLAIMS B	(German)	200542	1992
CLAIMS B	(French)	200542	2212
SPEC B	(English)	200542	6668
Total word count - document A			0
Total word count - document B			12823
Total word count - documents A + B			12823

...SPECIFICATION decrypt key.
According to one aspect of this embodiment, the encryption engine further includes W **look - up tables** for storing each of the possible W sets of permutations. According to a **different aspect** of this embodiment, the **encryption** engine further includes M<W **look - up tables** for storing M available sets of the possible W sets of permutations. According to a **different aspect** of this embodiment, the **encryption** engine further includes N<M<W **look - up tables** for storing N sets of permutations preselected from M available sets of the possible W...

...decrypt key.
According to one aspect of this embodiment, the encryption engine further includes W **look - up tables** for storing each of the possible W sets of permutations. According to a **different aspect** of this embodiment, the **encryption** engine further includes M<W **look - up tables** for storing M available sets of the possible W sets of permutations. According to a **different aspect** of this embodiment, the **encryption** engine further includes N<M<W **look - up tables** for storing N sets of permutations preselected from M available sets of the possible W...

18/3,K/17 (Item 17 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01116162
DEVICE AND METHOD FOR EVALUATING RANDOMNESS OF FUNCTION, DEVICE AND METHOD FOR GENERATING RANDOM FUNCTION, AND RECORDED MEDIUM ON WHICH PROGRAMS FOR IMPLEMENTING THESE METHODS ARE RECORDED
VORRICHTUNG UND VERFAHREN ZUM AUSWERTEN DER ZUFALLSVERTEILUNG EINER FUNKTION, VORRICHTUNG UND VERFAHREN ZUR ERZEUGUNG EINER ZUFALLSFUNKTION UND AUFZEICHNUNGSMEDIUM AUF WELCHEM PROGRAMME ZUR AUSFUHRUNG DIESER VERFAHREN AUFGEZEICHNET SIND.
DISPOSITIF ET PROCEDE D'EVALUATION DU CARACTERE ALEATOIRE D'UNE FONCTION, DISPOSITIF ET PROCEDE DE PRODUCTION D'UNE FONCTION ALEATOIRE ET SUPPORT ENREGISTRE SUR LEQUEL DES PROGRAMMES DE MISE EN APPLICATION DE CES

PROCEDES SONT ENREGISTRES
PATENT ASSIGNEE:
Nippon Telegraph and Telephone Corporation, (2460170), 19-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-8019, (JP), (Applicant designated States: all)
INVENTOR:
MORIAI, Shiho, 1-21-1-701, Kamioooka-higashi, Kounan-ku, Yokohama-shi, Kanagawa 233-0001, (JP)
AOKI, Kazumaro, 4-22-1-A-503, Kamariya-higashi, Kanazawa-ku, Yokohama-shi, Kanagawa 236-0042, (JP)
KANDA, Masayuki, D-401, 9-2-12, Sugita, Isogo-ku, Yokohama-shi, Kanagawa 235-0033, (JP)
TAKASHIMA, Youichi, 2-30-21, Kamariya-nishi, Kanazawa-ku, Yokohama-shi, Kanagawa 236-0046, (JP)
OHTA, Kazuo, 2-10-34, Yamanone, Zushi-shi, Kanagawa 249-0002, (JP)
LEGAL REPRESENTATIVE:
Hoffmann, Eckart, Dipl.-Ing. (5571), Patentanwalt, Bahnhofstrasse 103, 82166 Grafelfing, (DE)
PATENT (CC, No, Kind, Date): EP 1001569 A1 000517 (Basic)
WO 9963706 991209
APPLICATION (CC, No, Date): EP 99922630 990601; WO 99JP2924 990601
PRIORITY (CC, No, Date): JP 98153066 980602
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS (V7): H04L-009/06; G09C-001/00
ABSTRACT WORD COUNT: 120
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200020	4694
SPEC A	(English)	200020	6270
Total word count - document A			10964
Total word count - document B			0
Total word count - documents A + B			10964

...SPECIFICATION from an example cited in literature "T. Jakobsen, L. R. Knudsen, 'The Interpolation Attack on **Block** Cipher,' Fast **Software Encryption** Workshop (FSE4) (Lecture Notes in Computer Science 1267), pp. 28-40, Springer-Verlag, 1997," it...

...readily cryptanalyzed by the higher order and the interpolation cryptanalysis in the case where the **S - box** is **formed** by a function of a certain algebraic structure selected as a function resistant to the ...

18/3,K/18 (Item 18 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01085255
Cryptographic Processing apparatus, cryptographic processing method and storage medium storing cryptographic processing program for realizing high-speed cryptographic processing without impairing security
Vorrichtung und Verfahren zur kryptographischen Verarbeitung sowie Aufzeichnungsmedium zum Aufzeichnen eines kryptographischen Verarbeitungsprogramms zur Ausfuhrung einer schnellen kryptographischen Verarbeitung ohne Preisgabe der Sicherheit
Dispositif et procede de traitement cryptographique ainsi que support d'enregistrement pour stocker un programme de traitement cryptographique afin de realiser un traitement cryptographique rapide sans compromettre la securite
PATENT ASSIGNEE:

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (1855503), 1006, Oaza Kadoma, Kadoma-shi, Osaka 571, (JP), (Proprietor designated states: all)
INVENTOR:
Ohmori, Motoji, 1-9-3-402, Nasuzukuri, Hirakata-shi, Osaka-fu 573-0071, (JP)
Yokota, Kaoru, 3-9-202, Shinnozukacho, Ashiya-shi, Hyogo-ken 659-0016, (JP)
LEGAL REPRESENTATIVE:
Butcher, Ian James et al (79251), A.A. Thornton & Co. 235 High Holborn, London WC1V 7LE, (GB)
PATENT (CC, No, Kind, Date): EP 954135 A2 991103 (Basic)
EP 954135 A3 000607
EP 954135 B1 040407
APPLICATION (CC, No, Date): EP 99303133 990422;
PRIORITY (CC, No, Date): JP 98116758 980427; JP 98116759 980427
DESIGNATED STATES: DE; FR; GB; IT
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
ABSTRACT WORD COUNT: 220
NOTE:
Figure number on first page: 7

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199944	5394
CLAIMS B	(English)	200415	2552
CLAIMS B	(German)	200415	2400
CLAIMS B	(French)	200415	3062
SPEC A	(English)	199944	15316
SPEC B	(English)	200415	9840
Total word count - document A			20714
Total word count - document B			17854
Total word count - documents A + B			38568

...SPECIFICATION cipher, when receiving 64-bit actual key data from the key controlling unit 604. The **substitution table** data **generating** unit 602 then outputs the **generated substitution table** data to the data encrypting unit 601.
The input key generating unit 603 stores 64...

...and the stored 64-bit actual key data and outputs the result to the data **encrypting** unit 601 as input key data for **encryption** of the **next** plaintext **block** . Since there is no ciphertext block when the first plaintext block is to be encrypted...

...of encrypting plaintext block P0.
The substitution table data generating unit 602 in Fig. 14 **generates substitution table** data TG(K(0)) from actual key data K(0) received from the key controlling...

...the data encrypting unit 601.
The data encrypting unit 601 encrypts plaintext block P0 using **substitution** table data TG(K(0)) and input key data K(0)(+)IV to generate ciphertext block C0.
(2) **Next** , plaintext **block** P1 is **encrypted** as follows.
Since the key controlling unit 604 does not output new actual key data, the **substitution table** data **generating** unit 602 does not **generate** new **substitution table** data.
The input key **generating** unit 603 performs an exclusive-OR operation for corresponding bits in actual key data K...

18/3,K/19 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00643663
Quantized coherent rake receiver for CDMA signals
Quantisierter koharenter RAKE-Empfanger fur CDMA-Signale
Recepteur RAKE coherent et quantifie pour signaux AMDC
PATENT ASSIGNEE:
  Ericsson Inc., (2648086), 6300 Legacy Drive, MS EVW 2-C-2, Plano, TX 75024, (US), (Proprietor designated states: all)
INVENTOR:
  Dent, Paul W., Apartment 201 F, Hyde Park Court, Cary, North Carlina 27513, (US)
LEGAL REPRESENTATIVE:
  Kuhn, Friedrich Heinrich (143302), Ericsson AB Patent Unit Radio Networks , 164 80 Stockholm, (SE)
PATENT (CC, No, Kind, Date): EP 622909 A2 941102 (Basic)
EP 622909 A3 000719
EP 622909 B1 040714
APPLICATION (CC, No, Date): EP 94850071 940428;
PRIORITY (CC, No, Date): US 54028 930429
DESIGNATED STATES: DE; ES; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04B-007/005; H04B-001/66
ABSTRACT WORD COUNT: 212
NOTE:
  Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	1612
CLAIMS B	(English)	200429	1189
CLAIMS B	(German)	200429	1086
CLAIMS B	(French)	200429	1407
SPEC A	(English)	EPABF2	9728
SPEC B	(English)	200429	9818
Total word count - document A			11342
Total word count - document B			13500
Total word count - documents A + B			24842

...SPECIFICATION binary bits, and these bit blocks are encoded with error correcting orthogonal (or bi-orthogonal) **block codes** . The orthogonal 2(sup(M)-bit **block code** -words are **scrambled** by modulo-2 N-bit addition of a scrambling mask that may be retrieved from a **look - up table** in a memory. In the case of ideal scrambling masks, there may be either n...

...SPECIFICATION binary bits, and these bit blocks are encoded with error correcting orthogonal (or bi-orthogonal) **block codes** . The orthogonal 2M)-bit block codewords are **scrambled** by modulo-2 N-bit addition of a scrambling mask that may be retrieved from a **look - up table** in memory. In the case of ideal scrambling masks, there may be either nA))=N1...

18/3,K/20 (Item 20 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00576855
Multiple access coding for radio communication
Vielfachzugriffskodierung fur Funkubertragung
Codage d'acces multiple pour un systeme de transmission par radio
PATENT ASSIGNEE:
  ERICSSON INC., (1203496), P.O. Box 13969, 1 Triangle Drive, Research Triangle Park, N.C. 27709, (US), (Proprietor designated states: all)

INVENTOR:
  Dent, Paul W., Apartment 201 F, Hyde Park Court, Cary, North Carolina 27513, (US)
  Bottomley, Gregory E., 100 Merlot Court, Cary, NC 27511, (US)
LEGAL REPRESENTATIVE:
  Wennerholm, Kristian et al (24462), Ericsson Radio Systems AB, Patent Unit Radio Access, 164 80 Stockholm, (SE)
PATENT (CC, No, Kind, Date): EP 565506 A2 931013 (Basic)
EP 565506 A3 940525
EP 565506 B1 010718
APPLICATION (CC, No, Date): EP 93850068 930401;
PRIORITY (CC, No, Date): US 866865 920410
DESIGNATED STATES: DE; ES; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04J-013/00; H04B-001/66; H04L-009/00; H04J-011/00
ABSTRACT WORD COUNT: 174
NOTE:
  Figure number on first page: 7

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	3548
CLAIMS B	(English)	200129	3670
CLAIMS B	(German)	200129	3507
CLAIMS B	(French)	200129	4503
SPEC A	(English)	EPABF1	14079
SPEC B	(English)	200129	14057
Total word count - document A			17629
Total word count - document B			25737
Total word count - documents A + B			43366

...SPECIFICATION 50, and these bit blocks are encoded by an error correction orthogonal (or bi-orthogonal) **block coder** 52. The orthogonal 2(sup(M)-bit block codewords are **scrambled** by a modulo-2 N-bit adder 53 with a scrambling mask, constructed as described above, retrieved from a **look - up table** in a memory 60. In the case of ideal scrambling masks, there are either n...

...SPECIFICATION 50, and these bit blocks are encoded by an error correction orthogonal (or bi-orthogonal) **block coder** 52. The orthogonal 2M)-bit block codewords are **scrambled** by a modulo-2 N-bit adder 53 with a scrambling mask, constructed as described above, retrieved from a **look - up table** in a memory 60. In the case of ideal scrambling masks, there are either nA...

18/3,K/21 (Item 21 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00395937
Method for enciphering a series consisting of at least one symbol.
Verfahren zum Verschlusseln einer Folge, die aus mindestens einem Symbol besteht.
Procede de chiffrage d'une serie consistant d'au moins un symbole.
PATENT ASSIGNEE:
  Koninklijke PTT Nederland N.V., (1066890), P.O. Box 95321, NL-2509 CH The Hague, (NL), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
  Boly, Jean Paul, 22 Loethe, NL-2381 BL Zoeterwoude, (NL)
  Roelofsen, Gerrit, 58 Drossaardslag, NL-2805 DD Gouda, (NL)
PATENT (CC, No, Kind, Date): EP 399587 A1 901128 (Basic)
EP 399587 B1 940223

APPLICATION (CC, No, Date): EP 90201136 900521;
PRIORITY (CC, No, Date): NL 891323 890526
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04L-009/06;
ABSTRACT WORD COUNT: 249

LANGUAGE (Publication,Procedural,Application): English; English; Dutch
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	764
CLAIMS B	(German)	EPBBF1	666
CLAIMS B	(French)	EPBBF1	811
SPEC B	(English)	EPBBF1	3395
Total word count - document A			0
Total word count - document B			5636
Total word count - documents A + B			5636

...SPECIFICATION possible series of n symbols by a specific series of k symbols, where k > 0, **is generated** , and in which always a second series of k symbols which has a good statistical...

...the invention is characterized in that by means of a key at least one arbitrary **substitution table** is **generated** , which table substitutes each possible series of n symbols by a specific series of k **symbols** , where k > 0, and that a **second** series of **k** symbols, which series has **a** good statistical distribution, is combined **with one** of the two first-named series of symbols, to obtain an enciphered output series.
The invention is based on the understanding that the reliability of the substitution function used in **the** encipher algorithm will be augmented considerably, if both the transmitting party and the receiving party **create** one and the **same** arbitrary **S - box** on the basis of a secret key transmitted via a key channel, which involves of...

18/3,K/22 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00895845 **Image available**
DIGITAL VIDEO RECORDER EMPLOYING A FILE SYSTEM ENCRYPTED USING A PSEUDO-RANDOM SEQUENCE AND A UNIQUE ID
ENREGISTREUR VIDEO NUMERIQUE FAISANT APPEL A UN SYSTEME DE FICHIERS CRYPTES AU MOYEN D'UNE SEQUENCE PSEUDO-ALEATOIRE ET D'UN IDENTIFICATEUR UNIQUE
Patent Applicant/Assignee:
KEEN PERSONAL MEDIA INC, One Morgan, Irvine, CA 92618, US, US (Residence) , US (Nationality)
KEEN PERSONAL TECHNOLOGIES INC, One Morgan, Irvine, CA 92618, US, US (Residence), US (Nationality)
Inventor(s):
BOYLE William B, 25901 Astor Way, Lake Forest, CA 92630, US,
Legal Representative:
SHARA Milad G (agent), Western Digital Technologies, Inc., Intellectual Property Department - C2, 20511 Lake Forest Drive, Lake Forest, CA 92630, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200230028 A1 20020411 (WO 0230028)
Application: WO 2001US29506 20010918 (PCT/WO US0129506)
Priority Application: US 2000676633 20000930
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK
SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5251

Fulltext Availability:
Detailed Description

Detailed Description
... program.

In one embodiment, the plaintext key 18 comprises a plurality of segment keys for **encrypting** each **segment** of the plaintext video **program** , and the seed value generator 62 generates a corresponding seed value 64 for each segment...

...the input arguments x and y, and the segment seed value 64 is the result.

Lookup tables may also be employed for **generating** the segment keys, and the algorithm for computing the segment keys may be programmably updated...program.

In one embodiment, the plaintext key 18 comprises a plurality of segment keys for **encrypting** each **segment** of the plaintext video **program** , and the coefficient value generator 70 generates a set of coefficient values 72 for each...

...the input arguments x and y, and the segment coefficient values 72 are the result. **Lookup tables** may also be employed for **generating** the segment keys, and the algorithm for computing the segment keys may be progranimably updated...

18/3,K/25 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00880905 **Image available**
ENHANCED MODULE CHIPPING SYSTEM
AMELIORATIONS APPORTEES A UN SYSTEME DE PIRATAGE DE MODULE
Patent Applicant/Assignee:
AUDI PERFORMANCE & RACING, 1027-B Opelika Road, Auburn, AL 36830, US, US (Residence), US (Nationality)
Inventor(s):
AUGSBURGER Brett, 236 Kelly Lane, Auburn, AL 36830, US,
BURWELL Eddie, 1405 E. Olive Dr. S.E., Huntsville, AL 35380, US,
DUDEL Frank, 809 Watts Dr., Huntsville, AL 35380, US,
Legal Representative:
RUDD Andy (et al) (agent), Renner, Otto, Boisselle & Sklar, 1621 Euclid Ave., 19th Fl., Cleveland, OH 44115, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200214981 A2-A3 20020221 (WO 0214981)
Application: WO 2001US25386 20010814 (PCT/WO US0125386)
Priority Application: US 2000225196 20000814
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7143

Fulltext Availability:
Detailed Description

Detailed Description
... of input bits equaled the number of output bits, and the selection of the applicable **substitution table** 222a-222d is made based upon the duplicated input bits created by the expansion and permutation module 220.

0 The outputs of **substitution tables** 222a-222d are provided to a **second** permutation **module** 224. The **second** permutation **module** 224 performs simple bit **scrambling** , which ensures unique one-to-one mapping of the internal address of the memory 161...

18/3,K/26 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00852763 **Image available**
INFORMATION SECURITY METHOD AND SYSTEM
PROCEDE ET UN SYSTEME DE SECURITE DE L'INFORMATION
Patent Applicant/Assignee:
XTREAMLOK PTY LTD, Unit 5, 8 Miller Street, Murarrie, QLD 4172, AU, AU (Residence), AU (Nationality)
Inventor(s):
TUCKER David, Unit 5, 8 Miller Street, Murarrie, QLD 4172, AU,
CRUMP Matt A, 7/519 Tingal Road, Wynnum, QLD 4178, AU,
WITMANN Jerome, 17, rue Gustave Eiffel, F-62300 Lens, FR,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200186372 A2-A3 20011115 (WO 0186372)
Application: WO 2001IB1197 20010514 (PCT/WO IB0101197)
Priority Application: US 2000203877 20000512
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 12195

Fulltext Availability:
Detailed Description

Detailed Description
... present invention.

FIG. 12 is a table depicting an exemplary process that utilizes running line **encryption**

in accordance with **another aspect** of the present invention
FIG. 13 depicts an exemplary EIP **look - up table** in accordance with anotheri aspect of the present invention.

FIG. 14 depicts an exemplary import...

18/3,K/27 (Item 27 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00566889 **Image available**
APPARATUS AND METHOD FOR PERFORMING AND CONTROLLING ENCRYPTION/DECRYPTION FOR DATA TO BE TRANSMITTED ON LOCAL AREA NETWORK
DISPOSITIF ET PROCEDE SERVANT A EFFECTUER ET A COMMANDER UN CHIFFREMENT/DECHIFFREMENT DE DONNEES A TRANSMETTRE SUR UN RESEAU LOCAL
Patent Applicant/Assignee:
I-DATA INTERNATIONAL A S,
VIDECRANTZ Peter,
STEEN Sphiren,
STEENBERG Kim,
Inventor(s):
VIDECRANTZ Peter,
STEEN Sphiren,
STEENBERG Kim,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200030262 A2 **20000525** (WO 0030262)
Application: WO 99DK625 19991112 (PCT/WO DK9900625)
Priority Application: DK 981481 19981112; US 9860109743 19981124
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AT AU AZ BA BB BG BR BY CA CH CN CU CZ CZ DE DE DK DK EE EE
ES FI FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS
LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK SL TJ TM
TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY
KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 37626

Patent and Priority Information (Country, Number, Date):
Patent: ... **20000525**
Fulltext Availability:
Detailed Description
Claims

English Abstract
...a WAN: Wide Area Network). The data communication package contains a first section of non- **encrypted** data and a **second section** of **encrypted** data. The communication controller comprises a session key **LUT** unit (186), and a transmission and encryption section, which includes a data read transmission control...
Publication Year: **2000**

Detailed Description
... or WAN (wide area network), the data communication package containing a first section of non- **encrypted** data and a **second section** containing **encrypted** data, and comprising a session key **LUT** unit and a transmission and encryption section comprising.

(a) a data read transmission control unit...

...of a host
system and receiving input data therefrom and communicating with said

...host 1 0 system and receiving input data therefrom and communicating with said session key **LUT** (186), said session key LUT (186) providing a transmission
encryption key for said data communication...

...contained in said
1 5 second section of said data communication package,
(c) a data **encryption** unit (126) providing an **encryption** of said **second section** of said data communication package according to said transmission **encryption** key transferred from said session key **LUT** (1 86) to said data encryption unit
(126),
(d) an integrity check value calculation unit...
...package through communication with said network receiving controller (140),
and communicating with said session key **LUT** (186), said session key **LUT**
(1 86) providing a reception encryption key for said received data communication package,
(i) a...

...said received data communication package,
a data decryption unit (164) providing a decryption of said **second section** of
said received data communication package according to a reception **encryption** key transferred from said session key **LUT** (1 86) to said data
decryption unit (164),
(k) an integrity check value verification unit...WAN: Wide 0 Area Network), said data communication package containing a first section of non
encrypted data and a **second section** containing **encrypted** data, and said
communication controller comprising a session key **LUT** unit (186), and comprising:
(a) a data read transmission control unit (102) connected to a...

...of a host system and receiving input data therefrom and communicating with said session key **LUT** (1 86), said session key **LUT** (11 86) providing a transmission
encryption key for said data communication package,
(b) a data...

...input data contained in said
second section of said data communication package,
(c) a data **encryption** unit (126) providing an **encryption** of said **second section** of said data communication package according to said transmission **encryption** key transferred from said session key **LUT** (186) to said data encryption unit
(126)t
(d) an integrity check value calculation unit...

18/3,K/28 (Item 28 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00483537 **Image available**
IMPROVED BLOCK CIPHER METHOD
PROCEDE DE CHIFFREMENT BLOC AMELIORE
Patent Applicant/Assignee:
LUYSTER Frank C,
Inventor(s):
LUYSTER Frank C,

Patent and Priority Information (Country, Number, Date):
  Patent: WO 9914889 A1 **19990325**
  Application: WO 98US19255 19980916 (PCT/WO US9819255)
  Priority Application: US 9759142 19970917; US 9762992 19971023; US 9764331 19971030
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU
  IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
  PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW
  SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR
  IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 37707

Patent and Priority Information (Country, Number, Date):
  Patent: ... **19990325**
Fulltext Availability:
  Claims
Publication Year: **1999**

Claim
... and second linear operator are non-commutative with each other. CLAIM 5. The method of **encrypting** of claim I wherein the **sbox** is optimized so that **consecutive sections** of 20 bits or fewer are guaranteed to have at least a I bit output...

...each input bit difference. CLAIM 6. The method of encrypting of claim 1 wherein the **sbox** is optimized so that it has a guaranteed minimum number of bits of output difference...

18/3,K/29 (Item 29 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00439518 **Image available**
DATA SECURITY SYSTEM AND METHOD
SYSTEME ET PROCEDE DE SECURITE DE DONNEES
Patent Applicant/Assignee:
  REDCREEK COMMUNICATIONS INC,
  YIN John,
Inventor(s):
  YIN John,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9829982 A1 **19980709**
  Application: WO 97US24096 19971231 (PCT/WO US9724096)
  Priority Application: US 97778535 19970103
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU
  IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
  PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW
  SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE
  IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 8730

Patent and Priority Information (Country, Number, Date):
  Patent: ... **19980709**
Fulltext Availability:
  Detailed Description
Publication Year: **1998**

Detailed Description
... system for encryption and
decryption employing a conventional DES semiconductor chip;
Figures 2A-B are **block** diagrams illustrating, respectively, the
electronic **code** book (ECB) and cipher block chaining (CBC) block cipher
encryption modes of DES; Figure 3 is a block diagram illustrating in
more detail a portion...

...initial permutation of DES; Figure 5 is a block diagram illustrating an
expansion operation and **S - box**
operation of DES;
Figure 6 is a block diagram of a data security system in...

18/3,K/32 (Item 32 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00356431
CRYPTOGRAPHIC ACCESS AND LABELING SYSTEM
SYSTEME D'ACCES CRYPTOGRAPHIQUE ET D'ETIQUETAGE
Patent Applicant/Assignee:
KEYBYTE TECHNOLOGIES INC,
Inventor(s):
FOLLENDORE Roy D III,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9638945 A1 **19961205**
Application: WO 96US8851 19960603 (PCT/WO US9608851)
Priority Application: US 95489 19950601
Designated States:
(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)
AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP
KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD
SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD
RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG
CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 16663
Patent and Priority Information (Country, Number, Date):
Patent: ... **19961205**
Fulltext Availability:
Detailed Description
Publication Year: **1996**

Detailed Description
... To create the trailer, the data in data box 1022 are
provided to a Label **Element Encryption subroutine** 730 which
utilizes Spinup Randomizer subroutine 530 and a label **lookup**
table if irrational labels are desired. The spinup number and
25 the initializing vector for Spinup...

18/3,K/33 (Item 33 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00323160 **Image available**
MULTIPLE ACCESS CODING USING BENT SEQUENCES FOR MOBILE RADIO COMMUNICATIONS
CODAGE A ACCES MULTIPLE A L'AIDE DE SEQUENCES DE DEFORMATION POUR COMMUNICATIONS PAR RADIOTELEPHONES MOBILES
Patent Applicant/Assignee:
ERICSSON INC,
Inventor(s):

BOTTOMLEY Gregory E,
DENT Paul W,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9605668 A1 **19960222**
Application: WO 95US10229 19950811 (PCT/WO US9510229)
Priority Application: US 94291693 19940816
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TT UA UG UZ VN KE MW SD SZ UG AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 11526

Patent and Priority Information (Country, Number, Date):
Patent: ... **19960222**
Fulltext Availability:
Detailed Description
Publication Year: **1996**

Detailed Description
... scramble mask assigned. On the other hand, the whole set may be stored as a **look - up table** in a memory, in which case the number of bits
needed to address each mask...

...memory 60, that mask would
be retrieved from storage and modulo-2 added to the **block coded** signal

The ability selectively to address and retrieve a specific **scramble** mask becomes important in a subtractive CDMA system. For example, if stronger coded information signals...

18/3,K/34 (Item 34 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00277875
QUANTIZED COHERENT RAKE RECEIVER
RECEPTEUR RAKE COHERENT A QUANTIFICATION
Patent Applicant/Assignee:
ERICSSON GE MOBILE COMMUNICATIONS INC,
Inventor(s):
DENT Paul W,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9426051 A1 **19941110**
Application: WO 94US4820 19940429 (PCT/WO US9404820)
Priority Application: US 9354028 19930429
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU BR CA CN FI JP KR NZ
Publication Language: English
Fulltext Word Count: 12506

Patent and Priority Information (Country, Number, Date):
Patent: ... **19941110**
Fulltext Availability:
Detailed Description
Publication Year: **1994**

Detailed Description
... 20 bits, and these bit blocks are encoded with error correcting orthogonal (or bi-orthogonal) **block codes** , The orthogonal 2m@bit block codewords are **scrambled** by modulo@2 N@bit addition of a scrambling mask that may be retrieved from a **look - up table** in a memory.

25 In the case of ideal scrambling masks, there may be either...

18/3,K/35 (Item 35 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00275224
FINANCIAL TRANSMISSION SYSTEM
SYSTEME DE TRANSMISSION DE TRANSACTIONS FINANCIERES
Patent Applicant/Assignee:
SED STANDARDS ASSOCIATION INC,
SULLIVAN Mark K,
Inventor(s):
SULLIVAN Mark K,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9423400 A1 **19941013**
Application: WO 94US3344 19940328 (PCT/WO US9403344)
Priority Application: US 9338895 19930329
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AT AU BB BG BR BY CA CH CN CZ DE DK ES FI GB HU JP KP KR KZ LK LU LV MG MN MW NL NO NZ PL PT RO RU SD SE SI SK TT UA US UZ VN AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 12476
Patent and Priority Information (Country, Number, Date):
Patent: ... **19941013**
Fulltext Availability:
Detailed Description
Publication Year: **1994**

Detailed Description
... are generated by the device to avoid damage and discomfort to the listener's ear,
Another important **aspect** of the invention involves a method for **encrypting** the secret PIN code **portion** and/or the detectable **code** portion of the financial card. The method generally comprises the following steps.

programming a secret...

...a nonsecret identity offset into the device which corresponds to the master key; maintaining a **lookup table** associating the master key to the nonsecret identity offset at the device issuer location; generating...

18/3,K/37 (Item 37 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) . All rts. reserv.

00204897 **Image available**
ENCRYPTION SYSTEM FOR DIGITAL CELLULAR COMMUNICATIONS
SYSTEME DE CHIFFREMENT POUR LES COMMUNICATIONS CELLULAIRES NUMERIQUES

Patent Applicant/Assignee:
  ERICSSON GE MOBILE COMMUNICATIONS HOLDING INC,
Inventor(s):
  DENT Paul Wilkinson,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9202089 A1 **19920206**
  Application: WO 91US5087 19910718 (PCT/WO US9105087)
  Priority Application: US 90358 19900720
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AU BR CA GB JP KR
Publication Language: English
Fulltext Word Count: 13678

Patent and Priority Information (Country, Number, Date):
  Patent: ... **19920206**
Fulltext Availability:
  Detailed Description
Publication Year: **1992**

Detailed Description
... bit values
  generated are each a function of all of the selected key
  bits.

  In **another aspect** ,, the present invention includes a
  cellular communication system having an **encryption** subsystem
  which includes a key stream generator which uses a secret
  key to generate a...

...in two stages,
  First, the secret key is expanded in accordance with an
  algorithm to **produce** a **look up table** which is stored in
  memory. Second,, the circuit uses the count of a register
  along with the key in combination with the data stored in
  the **look up table** to **generate** a pseudo-random key stream
  which is mixed with the data before transmission. The
  system...

File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
(c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD=200648
(c) 2006 The Thomson Corporation

Set	Items	Description
S1	704	SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR SUBSTITUTION()TABLE? ?
S2	5918727	GOOD? ? OR ASSET? ? OR OBJECT? ? OR DATA OR INFORMATION OR CONTENT? ? OR FILE? ? OR DOCUMENT? ? OR ITEM? ? OR RECORD? ? OR ARTICLE? ?
S3	2011013	IMAGE? ? OR GRAPHIC? ? OR PICTURE? ? OR PHOTO? ? OR PHOTOGRAPH? ? OR JPEG OR JPG OR TIFF OR BITMAP
S4	2705650	MP3? ? OR MUSIC OR SONG? ? OR AUDIO OR NOISE OR MPEG OR QUICKTIME OR MOVIE? ? OR VIDEO? ? OR MPEG? ? OR FILM? ? OR MULTIMEDIA OR MEDIA
S5	550226	WEBPAGE? ? OR PAGE? ? OR TEMPLATE? ? OR CODE? ?
S6	705600	(PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)(3W)S2:S5
S7	26756	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR NEIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINING)(5W)S6
S8	37564	ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9	66	S8(5W)S7
S10	2	S1 AND S9
S11	10272758	(PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)
S12	537845	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR NEIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINING)(3W)S11
S13	14	S1 AND S8 AND S12
S14	12	S13 NOT S10
S15	6	S14 AND AC=US/PR AND AY=(1963:2000)/PR
S16	6	S14 AND AC=US AND AY=1963:2000
S17	6	S14 AND AC=US AND AY=(1963:2000)/PR
S18	4	S14 AND PY=1963:2000
S19	7	S15:S18

10/5,K/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0008265028 - Drawing available
WPI ACC NO: 1997-373140/
XRPX Acc No: N1997-309821
Inter-round mixing in iterated block substitution systems - using trickle and quick trickle permutations for inter round permutations of sub blocks or individual bits to obtain respectively row completeness or quasi row completeness in Latin squares
Patent Assignee: TELEDYNE ELECTRONIC TECHNOLOGIES (TDCO); TELEDYNE IND INC (TDCO)
Inventor: MITTENTHAL L
Patent Family (6 patents, 73 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 1997025799	A1	19970717	WO 1997US367	A	19970103	199734	B
AU 199721116	A	19970801	AU 199721116	A	19970103	199748	E
			WO 1997US367	A	19970103		
TW 337628	A	19980801	TW 1997102649	A	19970305	199849	E
US 5838794	A	19981117	US 1996584523	A	19960111	199902	E
US 5838795	A	19981117	US 1996584523	A	19960111	199902	E
			US 1997888454	A	19970707		
US 5838796	A	19981117	US 1996584523	A	19960111	199902	E
			US 1997888884	A	19970707		

Priority Applications (no., kind, date): US 1997888884 A 19970707; US 1997888454 A 19970707; US 1996584523 A 19960111

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 1997025799	A1	EN	125	14	

National Designated States,Original: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN
Regional Designated States,Original: AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

AU 199721116	A	EN	PCT Application WO 1997US367 Based on OPI patent WO 1997025799
TW 337628	A	ZH	
US 5838795	A	EN	Division of application US 1996584523
US 5838796	A	EN	Division of application US 1996584523

Alerting Abstract WO A1
The method of **encryption** involves receiving **successive blocks** of **data** , each being sub-divided into sub-blocks of data. Each sub-block is assigned to one of the individual **substitution boxes** . A statistically optimised permutation is selected.
It is determined if a set of preselected exponents is to be applied to the permutation. The set of preselected exponents is applied to the permutation if it is determined that a set of preselected exponents is to be applied, otherwise an exponent of one to the permutation is applied. After each round of encryption, an output of each numbered **substitution box** is applied as an input to the **substitution box** whose number is indicated by the permutation. The last two stages are repeated for a predetermined number of rounds.
USE/ADVANTAGE - Iterated block substitution system in which block **substitution tables** and pattern of inter round mixing are changed frequently. Interactions between sub blocks enhance mixing process and allow for inter round mixing in which sub blocks rather than individual blocks are permuted.

Title Terms/Index Terms/Additional Words: INTER; ROUND; MIX; BLOCK; SUBSTITUTE; SYSTEM; TRICKLE; QUICK; PERMUTATION; SUB; INDIVIDUAL; BIT; OBTAIN; RESPECTIVE; ROW; COMPLETE; QUASI; LATIN; SQUARE

Class Codes
International Classification (Main): H04L-009/00, H04L-009/06, H04L-009/28
US Classification, Issued: 380028000, 380029000, 380037000, 380042000, 380028000, 380037000, 380042000, 380028000, 380037000, 380042000

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A05

Alerting Abstract ...The method of **encryption** involves receiving **successive blocks** of **data** , each being sub-divided into sub-blocks of data. Each sub-block is assigned to one of the individual **substitution boxes** . A statistically optimised permutation is selected...

...to the permutation is applied. After each round of encryption, an output of each numbered **substitution box** is applied as an input to the **substitution box** whose number is indicated by the permutation. The last two stages are repeated for a...

...USE/ADVANTAGE - Iterated block substitution system in which block **substitution tables** and pattern of inter round mixing are changed frequently. Interactions between sub blocks enhance mixing...

Original Publication Data by Authority

Original Abstracts:
...permutation or a quasi quick trickle permutation to blocks of data allocated to n individual **substitution boxes** .

...

...permutation or a quasi quick trickle permutation to blocks of data allocated to n individual **substitution boxes** .

...

...quasi quick trickle permutation to the data bits undergoing block substitution allocated to n individual **substitution boxes** .

Claims:
...data, where n is an integer, each sub-block being assigned to one of n **substitution boxes** ;(b) selecting one of a quick trickle or a quasi quick trickle permutation as a...
...e)(1) is applied, applying a corresponding one of the sequence of permutations to the **substitution boxes** , assigning an output of each numbered **substitution box** as an input to the **substitution box** whose number is indicated by the corresponding one of the sequence of permutations, and if step (e)(2)is applied, applying the resulting permutation to the **substitution boxes** , assigning an output of each numbered **substitution box** as an input to the **substitution box** whose number is indicated by the resulting permutation;(g) repeating steps (e) and (f) for...

...of data, where n is an integer, the sub-block being assigned to n individual **substitution boxes** ;(b) selecting one of a quick trickle or a quasi quick trickle permutation as a...

...partially encrypted sub-blocks, assigning each partially encrypted sub-block as an input to the **substitution box** whose number is indicated by the the corresponding one of the sequence of permutations, and...

...partially encrypted sub-blocks, assigning each partially encrypted sub-block as an input to the **substitution box** whose number is indicated by the resulting kth permutation; and(g) repeating (e) and (f...
...divided into n sub-blocks of data, the sub-blocks being assigned to n individual **substitution boxes** ;(b) partially encrypting the n sub-blocks by assigning each of the n sub-blocks to one of n **substitution boxes** ;(c) reassembling the partially encrypted n sub-blocks into an m-bit block;(d) selecting...

10/5,K/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0005438973 - Drawing available
WPI ACC NO: 1991-038619/
XRPX Acc No: N1991-029817
Data enciphering system for computer - supplying successive data words to cipher circuit where each word is consecutively modified several times
Patent Assignee: TULIP COMPUTERS INT (TULI-N); TULIP COMPUTERS INT BV (TULI-N)
Inventor: KWAN B C T; VAN RUMPT H W; VANRUMPT H W
Patent Family (5 patents, 9 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 411712	A	19910206	EP 1990202092	A	19900731	199106	B
NL 198901983	A	19910301	NL 19891983	A	19890801	199113	E
US 5231662	A	19930727	US 1990560144	A	19900731	199331	E
			US 1991794326	A	19911112		
EP 411712	B1	19961002	EP 1990202092	A	19900731	199644	E
DE 69028748	E	19961107	DE 69028748	A	19900731	199650	E
			EP 1990202092	A	19900731		

Priority Applications (no., kind, date): NL 19891983 A 19890801
Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 411712	A	EN			
Regional Designated States,Original: BE DE ES FR GB IT NL SE					
US 5231662	A	EN	7	1	Continuation of application US 1990560144
EP 411712	B1	EN	12	1	
Regional Designated States,Original: BE DE DK ES FR GB IT NL SE					
DE 69028748	E	DE			Application EP 1990202092 Based on OPI patent EP 411712

Alerting Abstract EP A
The system enciphers all data words of e.g. 16 bits to be stored into a computer using a product cipher circuit includes alternately one from several permutation boxes (1-1 to 1-11) and one from a number of **substitution boxes** (1-12 to 1-51) each box being under the control of a specific part of a key.
The data words are enciphered in whole and the system can be regarded as a delay line. The data words can be combined with storage sector-specific coding words and with a key entered on an input device (2).
ADVANTAGE - Does not cause any delay that is noticeable to user. @(8pp Dwg.No.1/1)@

Equivalent Alerting Abstract US A
The method involves enciphering data words of a word width of n bits, in particular data words to be written in a computer storage. A product cipher circuit has alternately one from a number of permutation boxes with n inputs and n outputs and one from a plurality of **substitution boxes** with n inputs and n outputs. Each of these boxes is under the control of a specific part of an m-bits key. In the product cipher circuit the data

words are consecutively enciphered in whole and the enciphering device can be regarded as a delay line.

The data words to be enciphered can be combined with coding words which depend on the specific sector of the computer storage, in particular a hard storage disk unit, where the data words are stored. The sector-specific coding words and/or the m-bits key can be combined with a key to be entered by a user.

USE - E.g for data storage in computer memory.

Title Terms/Index Terms/Additional Words: DATA; ENCIPHER; SYSTEM; COMPUTER; SUPPLY; SUCCESSION; WORD; CIPHER; CIRCUIT; CONSECUTIVE; MODIFIED; TIME

Class Codes
International Classification (Main): H04L-009/06
(Additional/Secondary): G06F-012/14
US Classification, Issued: 380009000, 380029000, 380033000, 380037000, 380049000

File Segment: EPI;
DWPI Class: T01; U21; W01
Manual Codes (EPI/S-X): T01-D; T01-F09; T01-H01C; U21-A05D; W01-A05; W01-A06

Alerting Abstract ...from several permutation boxes (1-1 to 1-11) and one from a number of **substitution boxes** (1-12 to 1-51) each box being under the control of a specific part...

Equivalent Alerting Abstract ...of permutation boxes with n inputs and n outputs and one from a plurality of **substitution boxes** with n inputs and n outputs. Each of these boxes is under the control of...

Original Publication Data by Authority

Original Abstracts:
...of permutation boxes with n inputs and n outputs and one from a plurality of **substitution boxes** with n inputs and n outputs, each of these boxes being under the control of...

...of permutation boxes with n inputs and n outputs and one from a plurality of **substitution boxes** with n inputs and n outputs, each of these boxes being under the control of...
Claims:
...of permutation boxes with n inputs and n outputs and one from a plurality of **substitution boxes** with n inputs and n output, each of said permutation and **substitution boxes** being under the control of a specific part of the m-bit key, wherein each...

...words is permuted or substituted only once by each respective one of said permutation and **substitution boxes** and n and m are pre-defined integers; a modulo 2 adder wherein a first...

...of the deciphered n-bit words produced by said product cipher circuit with a next **successive** one of said **enciphered** n- **bit data** words to be deciphered in order to yield a current corresponding one of the deciphered...

File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
(c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD=200648
(c) 2006 The Thomson Corporation

Set	Items	Description
S1	5918727	GOOD? ? OR ASSET? ? OR OBJECT? ? OR DATA OR INFORMATION OR CONTENT? ? OR FILE? ? OR DOCUMENT? ? OR ITEM? ? OR RECORD? ? - OR ARTICLE? ?
S2	2011013	IMAGE? ? OR GRAPHIC? ? OR PICTURE? ? OR PHOTO? ? OR PHOTOG-RAPH? ? OR JPEG OR JPG OR TIFF OR BITMAP
S3	2705650	MP3? ? OR MUSIC OR SONG? ? OR AUDIO OR NOISE OR MPEG OR QU-ICKTIME OR MOVIE? ? OR VIDEO? ? OR MPEG? ? OR FILM? ? OR MULT-IMEDIA OR MEDIA
S4	550226	WEBPAGE? ? OR PAGE? ? OR TEMPLATE? ? OR CODE? ?
S5	7284634	PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR SEGMENT? ?
S6	4517377	FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR CHUNK? ?
S7	824961	(DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR N-EIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINI-NG OR SECOND??? OR 2ND)(3W)S5:S6
S8	37564	ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9	932459	S5:S6(5W)S1:S4
S10	398	S9(10N)S8(10N)S7
S11	110	S10 AND AC=US/PR AND AY=(1963:2000)/PR
S12	159	S10 AND AC=US AND AY=1963:2000
S13	158	S10 AND AC=US AND AY=(1963:2000)/PR
S14	148	S10 AND PY=1963:2000
S15	209	S11:S14
S16	51	S15 AND S9/TI
S17	51	IDPAT (sorted in duplicate/non-duplicate order)
S18	158	S15 NOT S17
S19	201	S9(10N)S8(10N)S7(10N)KEY? ?
S20	72	S18 AND S19
S21	72	IDPAT (sorted in duplicate/non-duplicate order)
S22	86	S18 NOT S21
S23	461	S8(5N)S7
S24	50	S22 AND S23
S25	36	S22 NOT S24
S26	7513	(S5:S6 OR PIECE)(3W)MESSAGE
S27	35	S8(10N)S26(10N)S7
S28	29	S27 NOT S15

28/3,K/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0015352740 - Drawing available
WPI ACC NO: 2005-703000/200572
Related WPI Acc No: 1996-518986; 1997-310156; 1998-009129; 1998-110064; 1998-286225; 1999-204782; 1999-444465; 2000-013122; 2000-194736; 2000-195398; 2000-365779; 2000-464989; 2000-490584; 2000-647035; 2001-022904; 2001-335855; 2001-357503; 2001-374044; 2001-397673; 2001-425330; 2001-570080; 2001-580828; 2001-581298; 2001-581665; 2001-595705; 2001-607222; 2002-011177; 2002-041658; 2002-062159; 2002-082807; 2002-154357; 2002-163652; 2002-179003; 2002-188040; 2002-205513; 2002-224088; 2002-226224; 2002-235400; 2002-236852; 2002-238406; 2002-238913; 2002-239839; 2002-256143; 2002-268672; 2002-315095; 2002-361599; 2002-361694; 2002-382444; 2002-391512; 2002-392708; 2002-393501; 2002-394013; 2002-405083; 2002-413035; 2002-416925; 2002-435593; 2002-479804; 2002-498079; 2002-498923; 2002-507125; 2002-507478; 2002-508021; 2002-528507; 2002-528580; 2002-556177; 2002-598690; 2002-617280; 2002-636862; 2002-654787; 2002-672857; 2002-673567; 2002-697772; 2002-698265; 2003-045908; 2003-056645; 2003-057552; 2003-067657; 2003-074123; 2003-091652; 2003-137905; 2003-140183; 2003-219596; 2003-237888; 2003-268467; 2003-327510; 2003-330044; 2003-353776; 2003-362315; 2003-362499; 2003-391983; 2003-401297; 2003-418353; 2003-418436; 2003-419661; 2003-465734; 2003-577429; 2003-586979; 2003-587433; 2003-615418; 2003-615425; 2003-655616; 2003-655715; 2003-656012; 2003-658647; 2003-689852; 2003-767701; 2003-777048; 2003-800216; 2003-800961; 2003-804783; 2003-829683; 2004-031964; 2004-041644; 2004-059948; 2004-119479; 2004-375604; 2004-386915; 2004-487761; 2004-624728; 2004-660515; 2004-698601; 2004-709696; 2004-795798; 2005-031214; 2005-038086; 2005-079360; 2005-110869; 2005-142700; 2005-259866; 2005-261577; 2005-521089; 2005-533060; 2005-617272; 2005-655503; 2005-689292; 2005-700681; 2005-776856; 2005-784522; 2005-793708; 2006-086183; 2006-115379; 2006-134064; 2006-134065; 2006-145508; 2006-163034; 2006-190576; 2006-190840; 2006-250572; 2006-391180; 2006-401355; 2006-432149
XRPX Acc No: N2005-576848

Message generation method for water marking applications, involves encrypting signature with common key and stenographically embedding encrypted signature in medium like printed or electronic objects

Patent Assignee: DIGIMARC CORP (DIGI-N); LEVY K L (LEVY-I); RAMOS D O (RAMO-I); RODRIGUEZ T F (RODR-I); SHARMA R K (SHAR-I)
Inventor: LEVY K L; RAMOS D O; RODRIGUEZ T F; SHARMA R K

Patent Family (3 patents, 107 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2005091547	A2	20050929	WO 2005US9072	A	20050318	200572	B
US 20050262351	A1	20051124	US 2004554543	P	20040318	200577	E
			US 200582217	A	20050315		
US 20050271246	A1	20051208	US 2002193719	A	20020710	200581	E
			US 2004554541	P	20040318		
			US 2004558767	P	20040331		
			US 200582179	A	20050315		

Priority Applications (no., kind, date): US 200582217 A 20050315; US 200582179 A 20050315; US 2002193719 A 20020710; US 2004554541 P 20040318; US 2004554543 P 20040318; US 2004558767 P 20040331

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2005091547	A2	EN	58	13	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW

MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SM SY TJ TM TN
TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
Regional Designated States,Original: AT BE BG BW CH CY CZ DE DK EA EE ES
FI FR GB GH GM GR HU IE IS IT KE LS LT LU MC MW MZ NA NL OA PL PT RO SD
SE SI SK SL SZ TR TZ UG ZM ZW

US 20050262351	A1	EN	Related to Provisional	US 2004554543
US 20050271246	A1	EN	C-I-P of application	US 2002193719
			Related to Provisional	US 2004554541
			Related to Provisional	US 2004558767

Original Publication Data by Authority

Original Abstracts:
...objects, audio and video). In one implementation, a message includes a first portion and a **second portion** . The first **portion** includes a first message and a first checksum, which are **encrypted** with a private key. The **encrypted** first portion is combined with the **second portion** . The **second portion** includes a second **message** and as second checksum. The combined **encrypted** first portion and the **second portion** form a signature. The signature is **encrypted** with a common or universal key, perhaps after error correction coding. The private key is...

...objects, audio and video). In one implementation, a message includes a first portion and a **second portion** . The first **portion** includes a first message and a first checksum, which are **encrypted** with a private key. The **encrypted** first portion is combined with the **second portion** . The **second portion** includes a second **message** and as second checksum. The combined **encrypted** first portion and the **second portion** form a signature. The signature is **encrypted** with a common or universal key, perhaps after error correction coding. The private key is...
Claims:
...A message generating method comprising:receiving a first message portion comprising a first checksum associated **therewith** ;encrypting the first message portion with a private key;receiving **a** second **message** portion comprising a second checksum associated therewith;combining **the** encrypted first **message** portion with **the second message** portion to yield a **signature** ;encrypting the signature with a common key; andsteganographically **embedding** the encrypted signature in media.

28/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0014715392 - Drawing available
WPI ACC NO: 2005-063009/
XRPX Acc No: N2005-054490
Transmitter for communication system, has encrypting **unit to** encrypt **first portion and first part of second** portion **of** message **package provided by message package provider, with** second part **of** second portion **used as** encrypting **key**
Patent Assignee: TRW INC (THOP)
Inventor: ALRABADY A I; JUZSWIK D L
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 6829357	B1	20041207	US 1999460061	A	19991214	200507 B

Priority Applications (no., kind, date): US 1999460061 A 19991214

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 6829357	B1	EN	10	6	

Transmitter for communication system, has encrypting **unit to** encrypt **first portion and first part of second** portion **of** message **package provided by message package provider, with** second part **of** second portion **used as** encrypting **key**

...NOVELTY - An **encrypting** unit **encrypts** the first portion and the first part of the **second portion** of a **message** package provided by a message package provider, with the **second part** of the **second portion** used as an **encrypting** key. An output unit outputs a signal to convey the **encrypted** first portion and **encrypted** first part of the **second portion** of the **message** package.

Original Publication Data by Authority

Original Abstracts:

...has a portion (b 28 /b) of a transmitter controller (b 14 /b) that provides a message package. An **encryption** portion (b 36 /b) of the controller (b 14 /b) **encrypts** a first **fraction** of the **message** package (e.g., a first **portion** of the **message** package and a first part of a second **portion** of the **message** package) using a second fraction of the message package (e.g., a second **part** of the **second portion** of the **message** package) as an **encryption** key. Transmitter components (b 32 /b and b 34 /b) output a signal (b 18 /b) that conveys the **encrypted** first **fraction** of the **message** package. Receiver components (b 56 /b and b 58 /b) receive the signal (b 18 /b). A decryption portion (b 60 /b) of...

Claims:

...is claimed: 4. A communication system comprising: means for providing a message package; means for **encrypting** a first **fraction** of the **message** package using a **second fraction** of the **message** package as an **encryption** key; means for outputting a signal that conveys the **encrypted** first **fraction** of the **message** package; means for receiving the signal; means for decrypting the signal using a decryption key...

...for encrypting the first portion and the first part of the second portion using the **second part** of the **second portion** as the encryption key, said means for outputting includes means for outputting the signal to convey the **encrypted** first portion and the **encrypted** first part of the **second portion** , and said means for reassembling includes means for assembling the **second portion** of the **message** package using the decryption key as the **second part** of the second portion of the message package, wherein said means for providing the message...

28/3,K/6 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

0014536139 - Drawing available

WPI ACC NO: 2004-718091/

XRPX Acc No: N2004-569242

Message transmission method for television, involves encrypting **two** portions **of** message **such that one portion is** encrypted **with high level and another** portion **of** message **is not** encrypted **or** encrypted **with low** encryption **level**

Patent Assignee: BROADCOM CORP (BROA-N)

Inventor: SESHADRI N

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20040193871	A1	20040930	US 2003457932	P	20030328	200470 B
			US 2004810688	A	20040329	

Priority Applications (no., kind, date): US 2003457932 P 20030328; US 2004810688 A 20040329

Patent Details
Number Kind Lan Pg Dwg Filing Notes
US 20040193871 A1 EN 21 4 Related to Provisional US 2003457932
Message transmission method for television, involves encrypting **two** portions **of** message **such that one portion is** encrypted **with high level and another** portion **of** message **is not** encrypted **or** encrypted **with low** encryption **level**
...NOVELTY - The one **portions** of **message** to be transmitted to receiver is **encrypted** with high **encryption** level and **another portion** of **message** is not **encrypted** or **encrypted** with low **encryption** level, in order to output to receiver.

Original Publication Data by Authority

Original Abstracts:
Particular **portions** of a **message** receive strong **encryption** while **other parts** of the **message** are less strongly **encrypted** or even unencrypted, resulting in a differentially **encrypted** data set. The data set is transmitted to a receiving end where it may be...
Claims:
...method of securely transmitting a message to a receiving device, comprising the steps of: (a) **encrypting** a first **part** of said **message** with a first level of **encryption** to produce a first message portion; (b) processing a **second part** of said **message** with a second level of **encryption** to produce a **second** message **portion** , with the second level of **encryption** selected from the group consisting of: (i) no encryption, and (ii) a level of encryption...

28/3,K/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2006 The Thomson Corporation. All rts. reserv.

0014009406 - Drawing available
WPI ACC NO: 2004-190798/200418
Related WPI Acc No: 2004-190792; 2004-190796; 2004-190797
XRPX Acc No: N2004-151449
Server-implemented message delivery method for electronic messaging, by encrypting at least first portion of message using split encryption key, and providing first key portion of split encryption key to another server
Patent Assignee: KARAMCHEDU M M (KARA-I); KRYPTIQ CORP (KRYP-N); SPONAUGLE J B (SPON-I)
Inventor: KARAMCHEDU M M; SPONAUGLE J B
Patent Family (4 patents, 104 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20040030918	A1	20040212	US 2002401945	P	20020807	200418	B
			US 2003394446	A	20030320		
WO 2004015943	A1	20040219	WO 2003US24540	A	20030806	200418	E
AU 2003258091	A1	20040225	AU 2003258091	A	20030806	200456	E
EP 1532783	A1	20050525	EP 2003784931	A	20030806	200535	E
			WO 2003US24540	A	20030806		

Priority Applications (no., kind, date): US 2002401945 P 20020807; US 2003394446 A 20030320

Patent Details
Number Kind Lan Pg Dwg Filing Notes
US 20040030918 A1 EN 25 12 Related to Provisional US 2002401945
WO 2004015943 A1 EN
National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ

NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW
AU 2003258091 A1 EN Based on OPI patent WO 2004015943
EP 1532783 A1 EN PCT Application WO 2003US24540
Based on OPI patent WO 2004015943
Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

...NOVELTY - The method involves, in a server (110), receiving, from another server, a request to **encrypt** at least a first **portion** of a **message** (70), generating a split **encryption** key comprising at least a first key portion and a **second** key **portion** , **encrypting** at least the first **portion** of the **message** using the split **encryption** key, and providing the first key portion to the other server.

Original Publication Data by Authority

Original Abstracts:
An enterprise-based system includes a storage server equipped to generate a split **encryption** key having at least a first key portion and a **second** key **portion** , that is used by the storage server to **encrypt** at least a **portion** of a **message** . Additionally, the first key portion of the split **encryption** key is retained by the storage server, while the **second** key **portion** of the split **encryption** key is delivered to a message routing server and is discarded from the storage server...

...An enterprise-based system includes a storage server equipped to generate a split **encryption** key having at least a first key portion and a **second** key **portion** , that is used by the storage server to **encrypt** at least a **portion** of a **message** . Additionally, the first key portion of the split **encryption** key is retained by the storage server, while the **second** key **portion** of the split **encryption** key is delivered to a message routing server and is discarded from the storage server...

...An enterprise-based system includes a storage server equipped to generate a split **encryption** key having at least a first key portion and a **second** key **portion** , that is used by the storage server to **encrypt** at least a **portion** of a **message** . Additionally, the first key portion of the split **encryption** key is retained by the storage server, while the **second** key **portion** of the split **encryption** key is delivered to a message routing server and is discarded from the storage server...
Claims:
...In a storage server, a method comprising:receiving from a second server, a request to **encrypt** a message;generating a split **encryption** key comprising at least a first key portion and a **second** key **portion** ; **encrypting** at least the first **portion** of the **message** using the split **encryption** key;providing the first key portion to the second server; anddiscarding first key portion...

28/3,K/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0014009400 - Drawing available
WPI ACC NO: 2004-190792/
Related WPI Acc No: 2004-190796; 2004-190797; 2004-190798
XRPX Acc No: N2004-151443
Secure message storage and sender-based notification generation for data processing, by generating message specific token comprising one or more encryption keys used to encrypt first portion of message

Patent Assignee: KARAMCHEDU M M (KARA-I); KRYPTIQ CORP (KRYP-N); MACHUCA L F (MACH-I); SPONAUGLE J B (SPON-I)
Inventor: KARAMCHEDU M M; KARMCHEDU M M; MACHUCA L F; SPONAUGLE J B
Patent Family (3 patents, 103 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20040030893	A1	20040212	US 2002401945	P	20020807	200418	B
			US 2003394410	A	20030320		
WO 2004015942	A1	20040219	WO 2003US24539	A	20030806	200418	E
AU 2003257194	A1	20040225	AU 2003257194	A	20030806	200456	E

Priority Applications (no., kind, date): US 2002401945 P 20020807; US 2003394410 A 20030320
Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20040030893	A1	EN	20	12	Related to Provisional US 2002401945
WO 2004015942	A1	EN			

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW
AU 2003257194 A1 EN Based on OPI patent WO 2004015942

...NOVELTY - The first portion of a message is stored on a server, and the complementary **second portion** of the message is stored on a client. The first **portion** of the **message** is **encrypted** and a message specific token comprising one or more **encryption** keys used to **encrypt** the first **portion** of the **message** is generated.

Original Publication Data by Authority

Original Abstracts:
...to store a first portion of a message, and a client to store a complementary **second portion** of the **message** . The first **portion** of the **message** is **encrypted** and a message specific token comprising one or more **encryption** keys used to **encrypt** the first **portion** of the **message** is generated. The **second portion** of the **message** stored on the client is subsequently combined with the message-specific token to form a...

...to store a first portion of a message, and a client to store a complementary **second portion** of the **message** . The first **portion** of the **message** is **encrypted** and a message specific token comprising one or more **encryption** keys used to **encrypt** the first **portion** of the **message** is generated. The **second portion** of the **message** stored on the client is subsequently combined with the message-specific token to form a...
Claims:
...comprising:storing a first portion of a message on a server, and storing a complementary **second portion** of the message on a client; **encrypting** the first portion of the message on the server, and generating a message specific token associated with the **encrypted** first **portion** of the **message** , the message-specific token comprising one or more **encryption** keys used to **encrypt** the first **portion** of the **message** ;combining the **second portion** of the **message** stored on the client with the message-specific token to form a partially secured message...

28/3,K/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0013403802 - Drawing available
WPI ACC NO: 2003-494092/200346
XRPX Acc No: N2003-392555

Content-level encryption protocol, for a digital content distribution system, that generates crypto-graphically protected digital data encoded content

Patent Assignee: IRDETO ACCESS BV (IRDE-N); MCLEAN I H (MCLE-I); WAJS A A (WAJS-I)
Inventor: MCLEAN I H; MCLEAN N H; WAJS A A

Patent Family (12 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2003052630	A2	20030626	WO 2002EP14828	A	20021218	200346	B
AU 2002364752	A1	20030630	AU 2002364752	A	20021218	200420	E
BR 200207375	A	20040615	BR 20027375	A	20021218	200440	E
			WO 2002EP14828	A	20021218		
US 20040139336	A1	20040715	WO 2002EP14828	A	20021218	200447	E
			US 2004468625	A	20040301		
EP 1456777	A2	20040915	EP 2002804920	A	20021218	200460	E
			WO 2002EP14828	A	20021218		
KR 2004068100	A	20040730	KR 2004701237	A	20040128	200475	E
CN 1524381	A	20040825	CN 2002805187	A	20021218	200477	E
ZA 200306420	A	20041229	ZA 20036420	A	20030818	200505	E
JP 2005513839	W	20050512	WO 2002EP14828	A	20021218	200532	E
			JP 2003553448	A	20021218		
MX 2004006196	A1	20041201	WO 2002EP14828	A	20021218	200561	E
			MX 20046196	A	20040621		
IN 200301274	P4	20051118	WO 2002EP14828	A	20021218	200607	E
			IN 2003CN1274	A	20030814		
HU 200501109	A1	20060328	WO 2002EP14828	A	20021218	200623	E
			HU 20051109	A	20021218		

Priority Applications (no., kind, date): US 2001342718 P 20011219

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2003052630	A2	EN	58	7	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SI SK SL SZ TR TZ UG ZM ZW

AU 2002364752	A1	EN		Based on OPI patent WO 2003052630
BR 200207375	A	PT		PCT Application WO 2002EP14828
				Based on OPI patent WO 2003052630
US 20040139336	A1	EN		PCT Application WO 2002EP14828
EP 1456777	A2	EN		PCT Application WO 2002EP14828
				Based on OPI patent WO 2003052630

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

ZA 200306420	A	EN	64	
JP 2005513839	W	JA	38	PCT Application WO 2002EP14828
				Based on OPI patent WO 2003052630
MX 2004006196	A1	ES		PCT Application WO 2002EP14828
				Based on OPI patent WO 2003052630
IN 200301274	P4	EN		PCT Application WO 2002EP14828
HU 200501109	A1	HU		PCT Application WO 2002EP14828
				Based on OPI patent WO 2003052630

Original Publication Data by Authority

Original Abstracts:
...and at least one further message section. At least one of the message sections is **encrypted** in such a way asto be decryptable independently of the **other** message **sections** . The **encrypted** **message** is assembled by adding a resynchronisation marker, separating a message section from an adjacentmessage section...

...first and at least one further message section. At least one of the message sections **is** encrypted in such a way as to be decryptable independently of **the** other **message** sections. **The** **encrypted** message is assembled by adding a resynchronisation marker, separating a **message** section from **an** **adjacent** **message** section and including explicit synchronisation information, to at least the further message sections...

...first and at least one further message section. At least one of the message sections **is** encrypted in such a way asto be decryptable independently of **the** other **message** sections. **The** **encrypted** message is assembled by adding a resynchronisation marker, separating a message section from an adjacentmessage...
Claims:
...the message sections is encrypted in such a way as to be decryptable independently of **the** other **message** sections, and wherein **the** encrypted message is assembled by adding a resynchronisation marker, separating a **message** section from **an** **adjacent** **message** section and including explicit synchronisation information, to at least the further message sections.

28/3,K/15 **(Item 15 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

0013075677 - Drawing available
WPI ACC NO: 2003-155975/
XRPX Acc No: N2003-123074
Encryption key selection method for communication network e.g. internet, involves encrypting subsequent message data block using selected encryption key and transmitting over network
Patent Assignee: DISANTO F J (DISA-I); KRUSOS D A (KRUS-I)
Inventor: DISANTO F J; KRUSOS D A
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20020146118	A1	20021010	US 2001782860	A	20010214	200315 B

Priority Applications (no., kind, date): US 2001782860 A 20010214

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20020146118	A1	EN	9	3	

...NOVELTY - A data value is extracted from a message data **block** . A **subsequent** **message** data **block** is **encrypted** using a selected **encryption** key and transmitted over a network.

28/3,K/20 **(Item 20 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

0010375714 - Drawing available
WPI ACC NO: 2000-075082/
XRPX Acc No: N2000-058922
Encryption and decryption key arrangements for communications apparatus,

e.g. facsimile machines
Patent Assignee: CHANTILLEY CORP LTD (CHAN-N)
Inventor: HAWTHORNE W M
Patent Family (5 patents, 20 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
GB 2339121	A	20000112	GB 199814003	A	19980630	200007	B
WO 2000001110	A1	20000106	WO 1999GB2052	A	19990630	200009	E
EP 1099323	A1	20010516	EP 1999928133	A	19990630	200128	E
			WO 1999GB2052	A	19990630		
JP 2002519940	W	20020702	WO 1999GB2052	A	19990630	200246	E
			JP 2000557580	A	19990630		
GB 2339121	B	20030305				200318	E

Priority Applications (no., kind, date): GB 199814003 A 19980630

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
GB 2339121	A	EN	11	2	
WO 2000001110	A1	EN			
National Designated States,Original: JP US					
Regional Designated States,Original: AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1099323	A1	EN			PCT Application WO 1999GB2052 Based on OPI patent WO 2000001110
Regional Designated States,Original: DE ES FR GB IT					
JP 2002519940	W	JA	11		PCT Application WO 1999GB2052 Based on OPI patent WO 2000001110

Original Publication Data by Authority

Original Abstracts:
...to form a cypher key stream the characters of which are used in sequence to **encrypt** or decrypt **successive** characters (or **elements**) of a **message** .

...
...to form a cypher key stream the characters of which are used in sequence to **encrypt** or decrypt **successive** characters (or **elements**) of a **message** .

```
File   8:Ei Compendex(R) 1970-2006/Jul W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2006/Jun
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Aug 02
         (c) 2006 BLDSC all rts. reserv.
File   2:INSPEC 1898-2006/Jul W4
         (c) 2006 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2006/Apr W4
         (c)2006 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2006/Jul W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Jul W2
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 2006 The Thomson Corp
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Jul W5
         (c) 2006 The Thomson Corp
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Jul
         (c) 2006 The HW Wilson Co.
File 266:FEDRIP 2005/Dec
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2006/Jul W5
         (c) 2006 FIZ TECHNIK
File  56:Computer and Information Systems Abstracts 1966-2006/Jul
         (c) 2006 CSA.
File  60:ANTE: Abstracts in New Tech & Engineer 1966-2006/Jul
         (c) 2006 CSA.
File  62:SPIN(R) 1975-2006/Apr W3
         (c) 2006 American Institute of Physics
File 239:Mathsci 1940-2006/Sep
         (c) 2006 American Mathematical Society

Set     Items   Description
S1       2739   SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR
              SUBSTITUTION()TABLE? ?
S2   15846103   GOOD? ? OR ASSET? ? OR OBJECT? ? OR DATA OR INFORMATION OR
             CONTENT? ? OR FILE? ? OR DOCUMENT? ? OR ITEM? ? OR RECORD? ? -
             OR ARTICLE? ?
S3    3500097   IMAGE? ? OR GRAPHIC? ? OR PICTURE? ? OR PHOTO? ? OR PHOTOG-
             RAPH? ? OR JPEG OR JPG OR TIFF OR BITMAP
S4    5048403   MP3? ? OR MUSIC OR SONG? ? OR AUDIO OR NOISE OR MPEG OR QU-
             ICKTIME OR MOVIE? ? OR VIDEO? ? OR MPEG? ? OR FILM? ? OR MULT-
             IMEDIA OR MEDIA
S5    1287867   WEBPAGE? ? OR PAGE? ? OR TEMPLATE? ? OR CODE? ?
S6     436235   (PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? -
             OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEM-
             ENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)(3W)-
             S2:S5
S7      14068   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR N-
             EIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE
              OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINI-
             NG)(5W)S6
S8      50696   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9          5   S8(5W)S7
S10         0   S1 AND S9
S11  15192511   (PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? -
             OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEM-
             ENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)
S12    591552   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR N-
             EIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE
              OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINI-
             NG)(3W)S11
S13        97   S8(5N)S12
S14         1   S1 AND S13
```

S15	6	S9 OR S14
S16	5	RD (unique items)

16/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

07971317 E.I. No: EIP06169825853
Title: Selective encryption for H.264/AVC video coding
Author: Shi, Tuo; King, Brian; Salama, Paul
Corporate Source: Video and Image Processing, Analysis, and Communications (VIPAC) Lab Department of Electrical and Computer Engineering Indiana University - Purdue University, Indianapolis, Indianapolis, IN 46202, United States
Conference Title: Security, Steganography, and Watermarking of Multimedia Contents VIII
Conference Location: San Jose, CA, United States Conference Date: 20060116-20060119
Sponsor: Society for Imaging Science and Technology, IS and T; SPIE
E.I. Conference No.: 67030
Source: Proceedings of SPIE - The International Society for Optical Engineering Security, Steganography, and Watermarking of Multimedia Contents VIII - Proceedings of SPIE-IS and T Electronic Imaging v 6072 2006.
Publication Year: 2006
CODEN: PSISDG ISSN: 0277-786X
Article Number: 607217
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0604W4
Abstract: Due to the ease with which digital data can be manipulated and due to the ongoing advancements that have brought us closer to pervasive computing, the secure delivery of video and images has become a challenging problem. Despite the advantages and opportunities that digital video provide, illegal copying and distribution as well as plagiarism of digital audio, images, and video is still ongoing. In this paper we describe two techniques for securing H.264 coded video streams. The first technique, SEH264Algorithm1, groups the data into the following blocks of data: (1) a block that contains the sequence parameter set and the picture parameter set, (2) a block containing a compressed intra coded frame, (3) a block containing the slice header of a P slice, all the headers of the macroblock within the same P slice, and all the luma and chroma DC coefficients belonging to the all the macroblocks within the same slice, (4) a block containing all the ac coefficients, and (5) a block containing all the motion vectors. The first three are encrypted whereas the last two are not. The second method, SEH264Algorithm2, relies on the use of multiple slices per coded frame. The algorithm searches the compressed video sequence for start codes (0x000001) and then **encrypts** the **next** N **bits** of **data** . copy 2006 SPIE-IS&T. 17 Refs.
Descriptors: *Cryptography; Image coding; Data reduction; Image analysis; Copyrights; Algorithms; Parameter estimation; Set theory
Identifiers: Selective Encryption; Partial Encryption; H.264/AVC
Classification Codes:
723.2 (Data Processing); 902.3 (Legal Aspects); 731.1 (Control Systems); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications); 902 (Engineering Graphics; Engineering Standards; Patents); 731 (Automatic Control Principles & Applications); 921 (Applied Mathematics)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING); 90 (ENGINEERING, GENERAL); 73 (CONTROL ENGINEERING); 92 (ENGINEERING MATHEMATICS)

16/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

07552223 E.I. No: EIP05339294278
Title: Speech encryption system with a low bit rate coding algorithm for analogue transmission line
Author: Chisaki, Yoshifumi; Morinaga, Haruki; Kitajima, Katsutoshi; Koba, Mitsuhiro; Usagawa, Tsuyoshi
Corporate Source: Department of Computer Science Faculty of Engineering Kumamoto University, Kumamoto, 860-8555, Japan
Source: Acoustical Science and Technology v 26 n 4 July 2005. p 371-373
Publication Year: 2005
CODEN: ASTCDS ISSN: 1346-3969
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0508W4
Abstract: A speech encryption system with a low bit rate coding algorithm for analogue transmission was proposed. Six **encryption** keys were introduced to three **different blocks** to protect speech **information**. The signal generated by the coding block was encrypted and the encrypted signal was modulated with the synchronization sequence decided by encryption key. It was found that the encrypted signal can be passed though the analogue transmission line and used for an analogue storage such as tape recorder. (Edited abstract) 3 Refs.
Descriptors: *Cryptography; Speech; Signal encoding; Algorithms; Block codes; Digital to analog conversion; Tape recorders; Computer simulation; Data privacy; Security of data
Identifiers: Analogue transmission line; Speech information; Speech encryption; Coding algorithms
Classification Codes:
752.2.1 (Sound Recording Equipment)
751.5 (Speech); 716.1 (Information & Communication Theory); 723.1 (Computer Programming); 723.2 (Data Processing); 752.2 (Sound Recording); 723.5 (Computer Applications)
716 (Electronic Equipment, Radar, Radio & Television); 751 (Acoustics, Noise & Sound); 723 (Computer Software, Data Handling & Applications); 752 (Sound Devices, Equipment & Systems)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 75 (SOUND & ACOUSTICAL TECHNOLOGY); 72 (COMPUTERS & DATA PROCESSING)

16/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06572011 E.I. No: EIP03427684456
Title: XML Pool Encryption
Author: Geuer-Pollmann, Christian
Corporate Source: Inst. for Data Commun. Systems University of Siegen, 57068 Siegen, Germany
Conference Title: Proceedings of the ACM Workshop on XML Security 2002
Conference Location: Fairfax, VA, United States Conference Date: 20021122-20021122
Sponsor: ACM SIGACT
E.I. Conference No.: 61595
Source: Proceedings of the ACM Workshop on XML Security 2003.
Publication Year: 2003
ISBN: 1581136323
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0310W4
Abstract: This paper describes an alternative encryption method for XML which is capable to encrypt single XML Information Set items. It is able to hide the size and the existence of encrypted contents. As a result, it prevents a 'traffic analysis', i.e. it's analogous counterpart for documents. In 2001, the W3C launched the XML **Encryption** working group which, among **other** things, defined how to **encrypt portions** of XML

documents . The portion must always be a subtree or a consecutive sequence of sub-trees. On the other hand, XML Access Control allows more granular restrictions on what portions on an XML document a client is allowed to see: XML Access Control can remove an ancestor node from a document while leaving a descendant node in the document. This paper describes an encryption system which allows to have these 'deep children' in plaintext while having the ancestors encrypted, i.e. bringing the property from XML Access Control to XML Encryption. 9 Refs.
Descriptors: *XML; Cryptography; Data structures; Telecommunication traffic; Security of data; Information services
Identifiers: Data padding
Classification Codes:
723.2 (Data Processing); 903.4 (Information Services)
723 (Computer Software, Data Handling & Applications); 718 (Telephone & Other Line Communications); 903 (Information Science)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING); 90 (ENGINEERING, GENERAL)

16/5/4 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01691684 ORDER NO: AADMQ-36013
SECURITY ASPECTS OF SUBSTITUTION-PERMUTATION ENCRYPTION NETWORKS
Author: CHEN, ZHI-GUO
Degree: M.SC.
Year: 1998
Corporate Source/Institution: QUEEN'S UNIVERSITY AT KINGSTON (CANADA) (0283)
Adviser: STAFFORD TANARES
Source: VOLUME 37/04 of MASTERS ABSTRACTS.
PAGE 1241. 104 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL ; COMPUTER SCIENCE
Descriptor Codes: 0544; 0984
ISBN: 0-612-36013-X

This thesis investigates some security aspects of basic substitution-permutation **encryption** networks (SPNs). Compared to **other block** ciphers, SPNs have many desirable and predictable cryptographic properties which are very useful for the design and analysis of cryptosystems.

We start with an estimate and upper bound on the nonlinearity distribution of **s - boxes** which shows that low nonlinearities are very unlikely for large **s - boxes** . This further confirms the statement that large **s - boxes** have better cryptographic properties. In addition, we use statistical methods to measure the distance between SPNs and the ideal cipher. Based on the experimental results on XOR table distributions and supported by the results on nonlinearity, we show that SPNs converge to the ideal cipher with an increasing number of rounds. We also present a new differential-like attack which is easy to implement and outperforms the classical differential crypt-analysis on the basic SPN structure. In particular, it is shown that 64-bit SPNs with 8 x 8 **s - boxes** are resistant to our attack after 12 rounds. From the attack, it can be seen that the number of active **s - boxes** is very important. For a secure SPN, it is necessary to make the number of active **s - boxes** in the last round independent of the number of active **s - boxes** in previous rounds. In this respect, it is found that the number of active **s - boxes** in the last round becomes independent of the number of active **s - boxes** in the first round for basic SPNs with an increasing number of rounds. These experiments and the analytical results may be regarded as some evidence towards provable security for SPN cryptosystems.

16/5/5 (Item 1 from file: 2)

08463944 INSPEC Abstract Number: C2003-01-6130S-027

Title: Secure and selective dissemination of XML documents

Author(s): Bertino, E.; Ferrari, E.
Author Affiliation: Dipt. di Sci. dell'Informazione, Milan Univ., Italy

Journal: ACM Transactions on Information and Systems Security vol.5, no.3 p.290-331
Publisher: ACM,
Publication Date: Aug. 2002 Country of Publication: USA
CODEN: ATISBQ ISSN: 1094-9224
SICI: 1094-9224(200208)5:3L.290:SSDD;1-L
Material Identity Number: D380-2002-006
U.S. Copyright Clearance Center Code: 1094-9224/02/0800-0290$5.00
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)

Abstract: XML (Extensible Markup Language) has emerged as a prevalent standard for document representation and exchange on the Web. It is often the case that XML documents contain information of different sensitivity degrees that must be selectively shared by (possibly large) user communities. There is thus the need for models and mechanisms enabling the specification and enforcement of access control policies for XML documents. Mechanisms are also required enabling a secure and selective dissemination of documents to users, according to the authorizations that these users have. In this article, we make several contributions to the problem of secure and selective dissemination of XML documents. First, we define a formal model of access control policies for XML documents. Policies that can be defined in our model take into account both user profiles, and document contents and structures. We also propose an approach, based on an extension of the Cryptolope TM approach (Gladney and Lotspiech (1997)), which essentially allows one to send the same document to all users, and yet to enforce the stated access control policies. Our approach consists of **encrypting different portions** of the same **document** according to different encryption keys, and selectively distributing these keys to the various users according to the access control policies. We show that the number of encryption keys that have to be generated under our approach is minimal and we present an architecture to support document distribution. (25 Refs)

```
File 275:Gale Group Computer DB(TM) 1983-2006/Aug 02
         (c) 2006 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Aug 02
         (c) 2006 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2006/Aug 02
         (c) 2006 The Gale Group
File  16:Gale Group PROMT(R) 1990-2006/Aug 01
         (c) 2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2006/Aug 02
         (c)2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Aug 03
         (c) 2006 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2006/Aug 03
         (c) 2006 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2006/Aug W3
         (c) 2006 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Jul W4
         (c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2006/Aug 02
         (c) 2006 Dialog
File 369:New Scientist 1994-2006/Jul W2
         (c) 2006 Reed Business Information Ltd.

Set     Items   Description
S1      30669   SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR
              SUBSTITUTION()TABLE? ?
S2   27341953   GOOD? ? OR ASSET? ? OR OBJECT? ? OR DATA OR INFORMATION OR
             CONTENT? ? OR FILE? ? OR DOCUMENT? ? OR ITEM? ? OR RECORD? ? -
             OR ARTICLE? ?
S3    4059528   IMAGE? ? OR GRAPHIC? ? OR PICTURE? ? OR PHOTO? ? OR PHOTOG-
             RAPH? ? OR JPEG OR JPG OR TIFF OR BITMAP
S4    7366934   MP3? ? OR MUSIC OR SONG? ? OR AUDIO OR NOISE OR MPEG OR QU-
             ICKTIME OR MOVIE? ? OR VIDEO? ? OR MPEG? ? OR FILM? ? OR MULT-
             IMEDIA OR MEDIA
S5    3747096   WEBPAGE? ? OR PAGE? ? OR TEMPLATE? ? OR CODE? ?
S6     686504   (PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? -
             OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEM-
             ENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)(3W)-
             S2:S5
S7      41185   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR N-
             EIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE
              OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINI-
             NG OR SECOND??? OR 2ND)(5W)S6
S8     371455   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9         68   S8(5N)S7
S10         0   S1 AND S9
S11        38   S1(100N)S6(100N)S8
S12        26   RD  (unique items)
```

12/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02480723 SUPPLIER NUMBER: 71186619 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Deciphering the Advanced Encryption Standard -- The new AES offers a strong standard that will win over product vendors and systems users.(Technology Information)
Smith, Richard
Network Magazine, 96
March 1, 2001
ISSN: 1093-8001 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3830 LINE COUNT: 00318

... activities. Using the new algorithm, companies can build and deploy standalone products such as link **encryptors** . The same is true of cryptographically agile products using protocols such as IPSec that can...

...the National Bureau of Standards (NBS, the precursor to NIST) began its search for the **encryption** algorithm that became DES. The NBS relied on the National Security Agency (NSA, www.nsa.gov) to analyze the proposed standard. IBM submitted an **encryption** algorithm, Lucifer, as a candidate. The NSA recommended two changes, which the NBS accepted before...

...most attackers, costs were falling steadily, and Moore's Law meant that a 56-bit **encryption** key wouldn't last long.
The second NSA-proposed change was to the algorithm' **s** **S** - **boxes** . These tables described how the algorithm would substitute one set of bits for another. DES **encrypts** data by shuffling it around and substituting groups of bits according to the contents of the **S** - **boxes** , repeating this process 16 times. Each repetition is called a round.
However, some observers feared that changes to **S** - **boxes** could introduce a trap door, allowing an attacker to decrypt DES messages without testing all...

...fuel suspicions, NSA instructed IBM not to describe the criteria it used to design the **S** - **boxes** .
While worries about key size have come true, worries about DES's basic design haven...

...machine had dropped tenfold. In 1997, a team of thousands of volunteers cracked a DES- **encrypted** message by working in parallel for several months. And in 1998, a team sponsored by built-in constants, tables, and **S** - **boxes** . Unlike DES, NIST wouldn't base the AES selection on classified and otherwise unpublishable analyses...

12/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01977762 SUPPLIER NUMBER: 18624712 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Overload of bugs hampers Remote Desktop beta. (McAfee Associates Inc's Remote Desktop 2.0 remote-access beta software)(PC Week Netweek) (Software Review)(Evaluation)
Phillips, Ken
PC Week, v13, n34, pN1(3)
August 26, 1996
DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1724 LINE COUNT: 00138

... chat feature is enabled when a connection is made, but on one occasion the agent' **s** chat **box** got out of sync with the controller, losing a character, and on another we mistakenly typed in the other PC' **s**

chat **box** by remote control and confused the connection, forcing a disconnect. McAfee is investigating these bugs...

...the fonts unreadable. The thumbnail sketches of remote windows were also useful.
Remote Desktop includes **encryption** capability for keystrokes only and not for video data or file transfers. At press time, McAfee hadn't decided which **encryption** algorithm to use, but 40- **bit** **Data Encryption** Standard was included in our beta copy and would seem a likely choice, since it...

12/3,K/3 (Item 3 from file: 275)

01381005 SUPPLIER NUMBER: 09558889 (USE FORMAT 7 OR 9 FOR FULL TEXT)
DES file encryption. (US National Bureau of Standards Data Encryption Standard) (tutorial)
Miller, Tony
EXE, v5, n5, p20(4)
Oct, 1990
DOCUMENT TYPE: tutorial ISSN: 0268-6872 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2925 LINE COUNT: 00211

... the left block in the next round of the algorithm. The right block is then **encrypted** with the ciphering function and XORd with the left block to form the right block...

...Bits 1 to 4 give the column number. The numbers looked up in the S- **box** convert to 4-bit numbers in binary notation. The eight 4-bit blocks are then combined to give the required 32-bit block. Since the number selected from the **S - box** depends on all the bits in the 6-bit block the process will be reversible...

...XORd with the left block as shown in Figure 4.
There are 16 rounds of **encipherment** with the 16 different keys. Finally, the inverse of the initial permutation is applied to...

...user must make a positive decision (by pressing the Y key) to continue with the **encryption** .
If the decision is to continue, the list of 16 keys is generated from the...to be permuted directly into the keylist in the form of a 16 by 48- **bit** array.
The input **file** is then reopened for binary read and write and the function crypt...

...it (int *keys) used to **encrypt** the file, 8 characters at a time. The various bitwise manipulations can be handled directly...

...with array element values of 0 or 1. The binary/decimal conversions needed for the **S - boxes** are handled with look-up tables. The final conversion of **bit** arrays to ASCII **codes** is also handled with a look-up table.
It is important not to leave any...

...which could be accessed using toolkits or otherwise. It is also worth checking that the **encryption** has proceeded satisfactorily before overwriting the original file. SID first loads the **encrypted** file into a temporary file. It then checks that the original and temporary files are of the same length. If they are, it copies the **encrypted** file on top of the original file, overwrites the temporary file with garbage and then...

...unchanged and reports the problem to the user. With the Microsoft C

compiler, SID will **encrypt** or decrypt at around 1 KB/sec on a 386 PC.
To decrypt, all you...

12/3,K/4 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

03576457 Supplier Number: 110211473 (USE FORMAT 7 FOR FULLTEXT)
VOCAL Introduces Optimal CTR-AES, CBC-MAC-AES, and CCMP-AES Encryption Cores for 802.11i.
PR Newswire, pNA
Nov 17, 2003
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 311

The 802.11i Counter mode/CBC-MAC Protocol (CCMP) offers **encryption** and message authentication based on the Advanced **Encryption** Standard (AES). CCMP uses the Counter mode (CTR) in AES for data **encryption** and the Cipher **Block** Chaining-Message Authentication **Code** (CBC-MAC) in AES for message integrity.
VOCAL's CCMP hardware engine comes in two...

...integrated 802.11i and a general AES hardware core that supports CTR and CBC-MAC **encryption** modes that can be integrated easily into an embedded processor.
For an 802.11i solution, the target rate of 54 Mbps requires approximately 27k gates (9K logic, 4K RAM, 14K **SBOX** ROMS). The stream is **encrypted** or decrypted at 6.4 bits per cycle which requires ~8.5 million MIPS processor...

12/3,K/5 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

03468186 Supplier Number: 103669900 (USE FORMAT 7 FOR FULLTEXT)
Mitsui Sumitomo Insurance London Management Selects Single Platform Firewall/VPN/Web Access Appliance from Secure Computing to Secure Inbound and Outbound Internet Access.
Business Wire, p5042
June 19, 2003
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 858

... time alerts in one simple, cost-effective package. Secure's SoftRemote VPN client provides an **encrypted** connection for their remote users via the Internet without costly dial-up or leased lines...

...the Sidewinder G2 and SoftRemote firewall/VPN combination secure MSILM's inbound traffic, Secure Computing' **s** On- **Box** SmartFilter feature enables them to build and enforce their outbound Web-usage policy at the same time. SmartFilter' **s** On- **Box** technology allows them to run Web access filtering directly on the Sidewinder G2 Firewall, saving...

...List, updated continuously, accurately categorizes millions of Web sites into content groups, enabling MSILM to **block** objectionable Web **content** and prevent the downloading of MP3 and executable files that are not work related. Extremely...

12/3,K/6 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02427367 Supplier Number: 60019178 (USE FORMAT 7 FOR FULLTEXT)
Joint Development of Next-Generation Encryption Algorithm 'Camellia' by NTT and Mitsubishi Electric.
Business Wire, p0529
March 10, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1113

... be required to improve security. The block size of AES is 128 bits. The proposed **encryption** algorithm Camellia adopts has a block size of 128 bits and key sizes of 128...

...per second, which is more than twice the speed of DES.
Moreover, the substitution tables (**s - boxes**) are designed to be suitable for small hardware. The key schedule can share a **part** of **data** randomizing and the memory requirement for subkeys is reduced. As a result, Camellia encryption hardware...

...SC 27 and are aiming at adoption as a international standard.
Notes:
(1) Symmetric-key **encryption** algorithm
An algorithm that uses the same key for both **encryption** and decryption. Widely used to quickly **encrypt** large quantities of data in messages or files.
(2) Block size
The size of the...

...bits for a successor symmetric-key block cipher to improve security.
(3) AES
Literally "Advanced **Encryption** Standard." NIST is seeking to establish a successor symmetric-key block cipher to DES by 2001.
(4) DES
Literally "Data **Encryption** Standard." A symmetric-key **encryption** algorithm designated as the standard for **encryption** by the National Bureau of Standards (now NIST) in 1977. Still widely used for **encrypting** data sent between banks.
(5) Key length
Determines the total number of available keys. For...cipher
There are two kinds of symmetric-key encryption algorithm: block ciphers and stream ciphers. **Block** ciphers bundle **data** into blocks of a certain length and encrypt each **block** . Stream ciphers encrypt **data** bit by bit.
(8) Differential cryptanalysis and linear cryptanalysis
Currently, these techniques are the most...

12/3,K/7 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04734041 Supplier Number: 62751188 (USE FORMAT 7 FOR FULLTEXT)
Computers and Networks; Conditional access for DTV.(digital television)
Gilmer, Brad
Broadcast Engineering, pNA
Feb, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1126

... private key generated by the encoder is sent via an Entitlement Control Message (ECM) as **part** of the **MPEG** stream. This key can be changed as often as the user desires, even changing several **part** of the

MPEG stream. When a **scrambled** MPEG signal is received by a conditional access decoder, the box first checks the EMM...

...interest to you the DTV broadcaster? First, you should know that, technically speaking, you can **scramble** some or all of your DTV transmissions. Second, you can use either relatively simple fixed-key **scrambling** where everyone with a box is able to decode your signal, or you can use variable-key **scrambling** , giving you the capability of addressing each subscriber' **s box** individually. Third, if you opt for a variable-key system, you will need to create...good. We will use smart cards, and one smart card will plug into another vendor' **s box** . The ATSC standard specifies the **scrambling** method to be used as the DVD Common **Scrambling** Method, or Simulcrypt. Sounds good to me - we will use a common **scrambling** approach. However, that is as far as it goes.
Where does this leave us? If...

12/3,K/8 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04733714 Supplier Number: 62602690 (USE FORMAT 7 FOR FULLTEXT)
Computers & networkds: Conditional access for DTV.
Gilmer, Brad
World Broadcast Engineering, pNA
March, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1103

... private key generated by the encoder is sent via an Entitlement Control Message (ECM) as **part** of the **MPEG** stream. This key can be changed as often as the user desires, even changing several...

...this information is encoded in an Entitlement Management Message (EMM), which also is sent as **part** of the **MPEG** stream. When a **scrambled** MPEG signal is received by a conditional-access decoder, the box first checks the EMM...

...broadcaster, you should know that, technically speaking, some or all of DTV transmissions can be **scrambled** . Simple fixed-key **scrambling** can be used, either relatively, where everyone with a box is able to decode the signal, or variable-key **scrambling** can give you the capability of addressing each subscriber' **s box** individually. If you opt for a variable-key system, you will need to create and...good. We will use smart cards, and one smart card will plug into another vendor' **s box** . The ATSC standard also specifies the **scrambling** method to be used as the DVD Common **Scrambling** Method, or Simulcrypt. Sounds good to me; we will use a common **scrambling** approach. However, that is as far as it goes.
Where does this leave us? If...

12/3,K/9 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04593199 Supplier Number: 60047962 (USE FORMAT 7 FOR FULLTEXT)
Joint development of next-generation encryption algorithm "Camellia" by NTT and Mitsubishi Electric; Symmetric block cipher achieves high security and world' highest efficiency.
M2 Presswire, pNA
March 10, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1213

... be required to improve security. The block size of AES is 128 bits. The proposed **encryption** algorithm Camellia adopts ...second, which is more than twice the speed of DES.

Moreover, the substitution tables (s- **boxes**) are designed to be suitable for small hardware. The key schedule can share a **part** of **data** randomizing and the memory requirement for subkeys is reduced.

As a result, Camellia **encryption** hardware achieves a size of approximately 10Kgates, which is in the smallest class in the...SC 27 and are aiming at adoption as a international standard.

Notes

*1 Symmetric-key **encryption** algorithm An algorithm that uses the same key for both **encryption** and decryption. Widely used to quickly **encrypt** large quantities of data in messages or files.

*2 Block size The size of the 3 AES Literally "Advanced **Encryption** Standard." NIST is seeking to establish a successor symmetric-key block cipher to DES by 2001.

*4 DES Literally "Data **Encryption** Standard." A symmetric-key **encryption** algorithm designated as the standard for **encryption** by the National Bureau of Standards (now NIST) in 1977. Still widely used for **encrypting** data sent between banks.

*5 Key length Determines the total number of available keys. For... cipher There are two kinds of symmetric-key encryption algorithm: block ciphers and stream ciphers. **Block** ciphers bundle **data** into blocks of a certain length and encrypt each **block** . Stream ciphers encrypt **data** bit by bit.

*8 Differential cryptanalysis and linear cryptanalysis Currently, these techniques are the most...

12/3,K/10 (Item 1 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

12483785 Supplier Number: 135417838 (USE FORMAT 7 FOR FULLTEXT)

Who's minding the data store? Experts say encryption is a good idea for sensitive data at rest . . . and on the move.

Network World, p42
August 15, 2005
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; General Trade
Word Count: 1523

... of Medicare patient data shipped on standard IBM cartridges. These updates represent an additional 18G **bytes** of data
to be added to the CECS Medicare data collection, which totals more than 7T bytes.

Because the **data** includes sensitive personal and healthcare information, it naturally falls under the Health Insurance Portability
and...

...at protecting the privacy of medical records. This is the main reason Fusca looked
at **encryption** with security vendor Decru, which has since been acquired by Network Appliance . Given the nearly...
...million
that the center had received for ongoing research involving the data, Fusca says his **encryption** costs, which he estimated
at about $75,000, were well worth the investment.
Once the...

...data passes through a cluster of Decru
DataFort E-series appliances, where it is subsequently **encrypted** . Thus, CECS can maintain a fully **encrypted** library of more
than 7T **bytes** of Medicare **data** on tape. Fusca and his team have

also designed the CECS architecture, which includes Network
Appliance network storage, to take advantage of DataFort's combined access controls, authentication and **encryption** capabilities.
"Data now flows all through the system, **encrypted** up until the time it comes out on the user' **s** Linux **box** ," Fusca says. "The
process is totally transparent to the users, and there is no lag time in the processing of the data to their screen."
Fusca favors hardware-based **encryption** , largely because of his prior experiences with software-based approaches. "We'd been
through all those games before (with software-based **encryption**), and thought there had to be a better way to do **encryption** ,"
Fusca says. He was referring to prior challenges managing **encryption** keys, the ongoing risk of keys being compromised, and
the difficulty of synchronizing clients to...

...latest version.
Canadian accounting firm RSM Richter decided to use Application Security's DBEncrypt to **encrypt** a few SQL Server database
fields in its Microsoft Great Plains software-based human resources
...

12/3,K/11 (Item 2 from file: 16)

10141104 Supplier Number: 91916027 (USE FORMAT 7 FOR FULLTEXT)
Customized processor extension speeds network cryptology: collapsing several conventional instructions into one custom instruction yields a performance increase of 92x for 3DES. (Design Application: Software).
Davies, Peter; Robsky, Steve
Electronic Design, v50, n19, p83(4)
Sept 16, 2002
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2563

... as ciphertext. There are essentially three components to the DES algorithm. To encipher a 64- **bit** **data** block, the DES algorithm performs the following functions (Fig. 1):
1. Initial permutation (IP)
2...

...one clock cycle.
Sixteen iterations of this instruction would almost complete a 64-bit DES **encryption** routine. Additional instructions would perform the initial and final permutations on the data block and...
...algorithm is a bit-level permutation function often referred to as the switch-box or **S** - **box** function. By sequentially executing 16 iterations of this function, the algorithm **encrypts** a 64- **bit** **block** of **data** based on a 56-bit private key. It's difficult to implement the **S** - **box** permutation function with the logical operators typically found in general-purpose processors. The CPU must...

...analyzing the DES software, two counts of the processor cycles required for each stage of **encryption** were tabulated. The first (smaller) cycle-count number is for a processor with a barrel...

...32-bit reads from memory for every DES round--one for each of the eight S - **box** substitutions, and two to read the successively rotated 56-bit key from the 16-entry schedule. Because the data stream is effectively little-endian and the **encryption** algorithm is big-endian, the processor must swap the bytes while reading from and writing...

...custom extension registers and four custom instructions:

* Registers L and R would hold the 64- **bit** **data** block.
* Registers C and D would hold the 56-bit (2 x 28) key.
* Instruction...

12/3,K/12 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04529023 Supplier Number: 46654248 (USE FORMAT 7 FOR FULLTEXT)
Overload of bugs hampers Remote Desktop beta
PC Week, pN01
August 26, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1645

... chat feature is enabled when a connection is made, but on one occasion the agent' **s** chat **box** got out of sync with the controller, losing a character, and on another we mistakenly typed in the other PC' **s** chat **box** by remote control and confused the connection, forcing a disconnect. McAfee is investigating these bugs...

...the fonts unreadable. The thumbnail sketches of remote windows were also useful.
Remote Desktop includes **encryption** capability for keystrokes only and not for video data or file transfers. At press time, McAfee hadn't decided which **encryption** algorithm to use, but 40- **bit** **Data Encryption** Standard was included in our beta copy and would seem a likely choice, since it...

12/3,K/13 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

0019949002 SUPPLIER NUMBER: 79371437 (USE FORMAT 7 OR 9 FOR FULL TEXT)
A Discussion of Current and Potential Issues Relating to Information Security for Internet Communications.
Iyengar, Jagannathan V.
Global Competitiveness, 9, 1, 541
Annual, 2001
ISSN: 1071-0736 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 4393 LINE COUNT: 00363

... because a DRC does not store any of the user's session keys or private **encryption** keys, and is never given copies of messages sent.
If this is sounding complicated, consider...

...listed for sale. Now imagine a "lock box" on the "front door" of every message **encrypted** by a user, with a spare copy of the session key inside, and with the...

...also that the lock box can easily be locked by the user, but only the **encrypted** messages use the "front lock box" with their own private **encryption** keys. The lock box remains unused until someone loses his/her keys. Whoever lost the...

...set of lock box keys, plus the list of people and corporations using that DRC' **s** lock **box** services.
The advantage to this technology is that no one needs to escrow his private...

...conventional private key escrow proposals, which require users to send a

copy of their personal **encryption** key(s) to a central location, such as in a bank or other pubic escrow...

...of applications and computer platforms, unlike ad hoc application-specific schemes.
Standard RSA public key **encryption** technology is used for authentication of DRC's and escrowing of session keys, but only...

...which can then be used to decrypt the message. This technology provides backup recovery of **encrypted** messages or files for users who have lost or damaged their keys, corporations who have...

...version 3.2, which provides a Global Virtual Private Network (GVPN) by using the 56- **bit** **Data** Encryption Standard (DES) to encrypt the Internet Protocol layer of the communications stream among firewalls...

12/3,K/14 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

16602796 SUPPLIER NUMBER: 112084205 (USE FORMAT 7 OR 9 FOR FULL TEXT)
File transfer drives business: today's file transfer services aren't just more powerful and convenient than their predecessors: they can provide a competitive edge.(The Business of Print)
Core, Erin
Graphic Arts Monthly, 75, 12, 42(2)
Dec, 2003
ISSN: 1047-9325 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 853 LINE COUNT: 00071

... this way, the job can get started before the CSR even arrives in the morning."
PART OF THE BIG **PICTURE**
File transfer is but one part of a larger chain for printers, says Janice Reese...

...Direct IP, a content distribution server--which many prepress pundits refer to as Wam!Net' **s** "purple **box** "--sits at the customer's site, communicating over the latter's existing Internet connection to Wam!Net's private network using an **encrypted** tunnel. Two other Wam!Net services, Direct and Direct DV, also offer different types of...

12/3,K/15 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

15516194 SUPPLIER NUMBER: 94123078 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Encryption and securiy: the Advanced Encryption Standard: the Advanced Encryption Standard is gaining steam as a stronger alternative to the Data Encryption Standard. Next-generation applications will go beyond secure networking protocols to include smart cards and electronic-media-content protection. (how it works).
Allman, Stuart
EDN, 47, 24, 26(3)
Oct 31, 2002
ISSN: 0012-7515 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2080 LINE COUNT: 00178

... increasing key sizes not only offer a larger number of bits with which you can **scramble** the data, but also increase the complexity of the cipher algorithm.
The AES algorithm repeats its core a number of times, depending on

the **encryption** -key size. Just like DES, the AES algorithm refers to these loop repetitions as "rounds...contain a variable number of rounds, depending on the key size.
* Cipher text is the **encrypted** data.
* Plain text is the original unencrypted data.
* The AES algorithm expands the 128-, 192...

...bit key. The total size of the key schedule depends on the key size.
* An **S - box** , or **substitution box** , is a look-up table.
EXPANDING INTO A KEY SCHEDULE
The AES algorithm expands the initial **encryption** key into a ... are as follows:
* the "key" is stored as an array of bytes and contains the **encryption** key;
* "key ...bytes;
* "SubWord()" is a byte-by-byte substitution of a 32-bit word using the **S - box** look-up table; and
* "Rcon(i)" is a look-up-table value that the word...

12/3,K/16 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

12414842 SUPPLIER NUMBER: 63691442 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Media security thwarts temptation, permits prosecution.(Industry Trend or Event)
Dipert, Brian
EDN, 45, 13, 101
June 22, 2000
ISSN: 0012-7515 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 8362 LINE COUNT: 00707

... San Francisco, CA.
(C.) Herre, Jurgen, and Christian Neubauer, "Audio watermarking of MPEG-2 AAC **bit** streams," 108th **Audio** Engineering Society Convention, Feb 19 to 22, 2000, Paris.
(D.) Allamanche, Eric, and Jurgen Herre, "Compatible **scrambling** of compressed audio," Proceeds of the 1999 IEEE Workshop on Applications of Signal Processing to...

...Paltz, NY.
(E.) Allamanche, Eric, and Jurgen Herre "Secure delivery of compressed audio by compatible **bit** -stream **scrambling** ," 108th **Audio** Engineering Society Convention, Feb 19 to 22, 2000, Paris.
(F.) Cravotta, Nicholas, " **Encryption** : more than just complex algorithms," EDN, March 18, 1999, pg 105.
(G.) Schneier, Bruce, Applied...

...Source Code in C, Second Edition, ISBN # 0471117099, John Wiley & Sons, 1995.
BELATEDLY CLOSING PANDORA' **S BOX**
As Hollywood and the consumer-electronics companies drag their feet in finalizing the Secure Digital...

...safeguards. Efforts under way by a number of vendors strive to retrofit digital media with **encryption** and watermarking capabilities, but legal restrictions and potential hardware and software incompatibilities limit their success...

12/3,K/17 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

11988650 SUPPLIER NUMBER: 61432674 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Settling debts online: a new tool for E-mailers.
Perry, Joellen
U.S. News & World Report, 128, 15, 60
April 17, 2000
ISSN: 0041-5537 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 563 LINE COUNT: 00045

... minutes, an automated E-mail announcing, "You've got cash!" will arrive in your pal' **s** in- **box** . To claim the dough, the recipient registers at the PayPal site and chooses to transfer...

...watchdog like TRUSTe to be sure personal data aren't sold to marketers. Also check **encryption** levels. PayPal's 40- **bit** **encryption** **scrambles** **data** adequately, but eMoneyMail's 128-bit standard is more secure.

12/3,K/18 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

11324436 SUPPLIER NUMBER: 55685434 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Encryption's state of flux.(data encryption)
Neeley, DeQuendre
Security Management, 43, 8, 37(1)
August, 1999
ISSN: 0145-9406 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 570 LINE COUNT: 00049

... customer information and credit card numbers.
However, says Amer, "I'm not replacing the traditional **encryption** systems at large. They work pretty well. I'm looking for a niche where the ...

...University researcher, "is that the limitations of real world physical devices...open up a Pandora' **s** **box** against quantum cryptographic systems."
In addition, for this technique to work, data transmission must be contained to short distances, which may prove impractical. Finally, some critics say that traditional **encryption** schemes do enough to protect information and that the incremental security improvement offered by quantum...
...need exists, they note that supercomputers are reducing the time it takes to crack traditional **encryption** . It may not be that far into the future before technology will make decrypting high-strength **encryption** bits a simple task.

12/3,K/19 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2006 The Gale Group. All rts. reserv.

10973317 SUPPLIER NUMBER: 54329987 (USE FORMAT 7 OR 9 FOR FULL TEXT)
ENCRYPTION: more than just complex algorithms.
Cravotta, Nicholas
EDN, 44, 6, 105(1)
March 18, 1999
ISSN: 0012-7515 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 6019 LINE COUNT: 00485

... message. Many of the standards, such as S/MIME, are protocol definitions based on base **encryption** algorithms, such as DES, Triple-DES, and RC2 (Rivest's Cipher).
By far, the most widely used algorithm is DES, employing a 56-bit key on a 64- **bit** **data** block. It is possible, however, for a cracker to break

a DES cipher in less...

...to replace 56-bit DES with an algorithm using a larger key space. The Advanced **Encryption** Standard (AES) is the official successor to DES, but it won't be available until...

...standard offers several modes supporting three keys per transaction, as opposed to one, and alternates **encryption** and decryption.
In addition to standard algorithms such as DES, many proprietary schemes offering varying...

...substitution devices, are available. The difference among these algorithms is their mathematical bases: DES uses **S boxes** , public-key **encryption** uses large prime numbers, and several of the next-generation algorithms use modified Feistel networks...

...for their takes on such claims.
The open/proprietary issue takes a different angle with **encryption** technologies. Certainly, you can prove an algorithm weak by breaking it, but no known means...

12/3,K/20 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02936653 884762301
Who's minding the data store?
Hope, Michele
Network World v22n32 PP: 42-44 Aug 15, 2005
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 1769

...TEXT: at protecting the privacy of medical records. This is the main reason Fusca looked at **encryption** with security vendor Decru, which has since been acquired by Network Appliance. Given the nearly...

...million that the center had received for ongoing research involving the data, Fusca says his **encryption** costs, which he estimated at about $75,000, were well worth the investment.

Once the...

...data passes through a cluster of Decru DataFort E-series appliances, where it is subsequently **encrypted** . Thus, CECS can maintain a fully **encrypted** library of more than 7T **bytes** of Medicare **data** on tape. Fusca and his team have also designed the CECS architecture, which includes Network Appliance network storage, to take advantage of DataFort's combined access controls, authentication and **encryption** capabilities.

"Data now flows all through the system, **encrypted** up until the time it comes out on the user' **s** Linux **box** ," Fusca says. "The process is totally transparent to the users, and there is no lag time in the processing of the data to their screen."

Fusca favors hardware-based **encryption** , largely because of his prior experiences with software-based approaches. "We'd been through all those games before (with software-based **encryption**), and thought there had to be a better way to do **encryption** ," Fusca says. He was referring to prior challenges managing **encryption** keys, the ongoing risk of keys being compromised, and the difficulty of synchronizing clients to...

...latest version.

Canadian accounting firm RSM Richter decided to use Application security's

DBEncrypt to **encrypt** a few SQL Server database fields in its Microsoft Great Plains software-based human resources...

12/3,K/21 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02033630 53770010
Designing cryptography for the new century
Landau, Susan
Association for Computing Machinery. Communications of the ACM v43n5 PP: 115-120 May 2000
ISSN: 0001-0782 JRNL CODE: GACM
WORD COUNT: 3805

...TEXT: nonlinearity. In block-structured algorithms nonlinearity is frequently achieved by using look-up tables called **S - boxes** (for **substitution boxes**).

Cryptanalytic Attacks

The most serious attacks on block-structured algorithms to date are differential and...

...that a fixed input difference may, with high probability, generate a particular output difference. By **encrypting** pairs of plaintexts X, X' with prescribed bitwise difference OX = X if X', and seeing...
...by Japanese cryptographer Mitsuru Matsui, works by finding linear relationships between plaintext, ciphertext, and key **bits** that reveal **information** about the key.

The AES Candidates

AES candidates were due June, 15, 1998. Of the...

...permutation network (Serpent), and an algorithm that relies on finite field operations to construct the **S - box** (Rijndael). MARS and RC6 use multiplication to perform diffusion, but MARS multiplies key words by...

12/3,K/22 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01995038 50821338
Conditional access for DTV
Gilmer, Brad
Broadcast Engineering v42n2 PP: 48-50 Feb 2000
ISSN: 0007-1994 JRNL CODE: BRG
WORD COUNT: 1121

...TEXT: private key generated by the encoder is sent via an Entitlement Control Message (ECM) as **part** of the **MPEG** stream. This key can be changed as often as the user desires, even changing several...

...this information is encoded in an Entitlement Management Message (EMM) which is also sent as **part** of the **MPEG** stream. When a **scrambled** MPEG signal is received by a conditional access decoder, the box first checks the EMM...

...interest to you the DTV broadcaster? First, you should know that, technically speaking, you can **scramble** some or all of your DTV transmissions. Second, you can use either relatively simple fixed-key **scrambling** where everyone with a box is able to decode your signal, or you

can use variable-key **scrambling** , giving you the capability of addressing each subscriber' **s box** individually. Third, if you opt for a variable-key system, you will need to create...

...good. We will use smart cards, and one smart card will plug into another vendor' **s box** . The ATSC standard specifies the **scrambling** method to be used as the DVD Common **Scrambling** Method, or Simulcrypt. Sounds good to me - we will use a common **scrambling** approach. However, that is as far as it goes.

Where does this leave us? If...

12/3,K/23 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01871447 05-22439
Encryption's state of flux
Neeley, DeQuendre
Security Management v43n8 PP: 37 Aug 1999
ISSN: 0145-9406 JRNL CODE: SEM
WORD COUNT: 531

...TEXT: customer information and credit card numbers.

However, says Amer, "I'm not replacing the traditional **encryption** systems at large. They work pretty well. I'm looking for a niche where the...

...University researcher, "is that the limitations of real world physical devices...open up a Pandora' **s box** against quantum cryptographic systems."

In addition, for this technique to work, data transmission must be contained to short distances, which may prove impractical. Finally, some critics say that traditional **encryption** schemes do enough to protect information and that the incremental security improvement offered by quantum...
...need exists, they note that supercomputers are reducing the time it takes to crack traditional **encryption** . It may not be that far into the future before technology will make decrypting high-strength **encryption** bits a simple task.

(Graph Omitted)

12/3,K/24 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01119712 97-69106
Secrecy and authenticity
Balon, Brett
Records Management Quarterly v29n4 PP: 24-31 Oct 1995
ISSN: 1050-2343 JRNL CODE: RMQ
WORD COUNT: 5866

...TEXT: chipsets which are designed to encrypt and decrypt messages using a secret military algorithm. The **encryption** system will be used in the Defense Message System. This proposal has run into controversy...U.S. and 135 U.S. based cryptographic products. Many of these provide DES (Data **Encryption** Standard) and/or RSA (named for Rivest, Shamir & Adleman, the creators) capabilities. As well, **encryption** software including DES and RSA algorithms and the popular Pretty Good Privacy (PGP) secure message...

...the world.(9)

In 1977, the U.S. National Bureau of Standards proposed the Data **Encryption** Standard for use in unclassified U.S. government communications. It was developed by IBM and almost immediately was assailed for potential security problems. DES uses a 56 bit key to **encipher** 64 **bit** **data** blocks using both permutations and substitutions to aid overall security.

It was criticized on the grounds that 56 bits were not seen as providing adequate security and that the **substitution** **boxes** may have hidden trapdoors. It was argued that with this short a key, DES could...

...and fast and can be implemented in both hardware and software. The hardware implementations can **encrypt** data at several million bits per second. (12)

The RSA Scheme was developed as a public key **encryption** system which uses a modulus as the product of two large primes (i.e., more than 100 digits each). This allows a person to **encipher** a message using a public key and send it to another person who is able...

12/3,K/25 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

00505376 CMP ACCESSION NUMBER: EWN19920406S1543
HIGHLY PARALLELIZED ALGORITHM BOOSTS PERFORMANCE - Encryption IC speeds up conversions
JANNIS MOUTAFIS
ELECTRONIC WORLD NEWS, 1992, n 058, 14
PUBLICATION DATE: 920406
JOURNAL CODE: EWN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: technology
WORD COUNT: 400

... its performance to the use of a highly parallelized conversion algorithm. Block ciphers like Data **Encryption** Standard (DES) normally pass data sequentially through a set of permutations and substitutions (also referred...

...as a block cipher) as many as 16 times. In each round, half the 32- **bit** **block** of **data** passes through a set of so-called **S - boxes** , the basic elements in which the substitution of data takes place. The result is 16...
...encyrption and decryption. SuperCrypt, by contrast, uses only eight rounds in decryption and nine in **encrypt**ion .
Loadable boxes SuperCrypt is also the first commercially available **encryption** chip with loadable **substitution** **boxes** . That means it can easily be upgraded to accommodate future modifications in the industry -standard DES algorithm relating to the **S - boxes** .
The chip uses two data ports and one independent security-control port. The two data...

12/3,K/26 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

118471
Who's minding the data store?
Experts say encryption is a good idea for sensitive data at rest . . . and on the move.

Journal: Network World Page Number: 42
Publication Date: August 15, 05
Word Count: 1390 Line Count: 135

Text:
... of datato be added to the CECS Medicare data collection, which totals more than 7T **bytes** . Because the **data** includes sensitive personal and healthcare information, it naturally falls under the Health Insurance Portabilityand Accountability...

... aimed at protecting the privacy of medical records. This is the main reason Fusca lookedat **encryption** with security vendor Decru, which has since been acquired by Network Appliance . Given the nearly $11 millionthat the center had received for ongoing research involving the data, Fusca says his **encryption** costs, which he estimatedat about $75,000, were well worth the investment. Once the Medicare...
... the data passes through a cluster of DecruDataFort E-series appliances, where it is subsequently **encrypted** . Thus, CECS can maintain a fully **encrypted** library of morethan 7T **bytes** of Medicare **data** on tape. Fusca and his team have also designed the CECS architecture, which includes NetworkAppliance network storage, to take advantage of DataFort's combined access controls, authentication and **encryption** capabilities. "Data now flows all through the system, **encrypted** up until the time it comes out on the user' **s** Linux **box** ," Fusca says. "Theprocess is totally transparent to the users, and there is no lag time in the processing of the data to their screen." Fusca favors hardware-based **encryption** , largely because of his prior experiences with software-based approaches. "We'd beenthrough all those games before [with software-based **encryption**], and thought there had to be a better way to do **encryption** ,"Fusca says. He was referring to prior challenges managing **encryption** keys, the ongoing risk of keys being compromised, andthe difficulty of synchronizing clients to ensure...

... latest version. Canadian accounting firm RSM Richter decided to use Application Security's DBEncrypt to **encrypt** a few SQL Server databasefields in its Microsoft Great Plains software-based human resources system...

```
File 348:EUROPEAN PATENTS 1978-2006/ 200630
         (c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060727,UT=20060720
         (c) 2006 WIPO/Univentio

Set     Items   Description
S1       2992   SBOX OR SBOXES OR (S OR SUBSTITUTI???)(1W)(BOX OR BOXES) OR
             SUBSTITUTION()TABLE? ?
S2    2021337   GOOD? ? OR ASSET? ? OR OBJECT? ? OR DATA OR INFORMATION OR
             CONTENT? ? OR FILE? ? OR DOCUMENT? ? OR ITEM? ? OR RECORD? ? -
             OR ARTICLE? ?
S3     660051   IMAGE? ? OR GRAPHIC? ? OR PICTURE? ? OR PHOTO? ? OR PHOTOG-
             RAPH? ? OR JPEG OR JPG OR TIFF OR BITMAP
S4     811644   MP3? ? OR MUSIC OR SONG? ? OR AUDIO OR NOISE OR MPEG OR QU-
             ICKTIME OR MOVIE? ? OR VIDEO? ? OR MPEG? ? OR FILM? ? OR MULT-
             IMEDIA OR MEDIA
S5     542967   WEBPAGE? ? OR PAGE? ? OR TEMPLATE? ? OR CODE? ?
S6     384277   (PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? -
             OR SEGMENT? ? OR FRACTION? ? OR ASPECT? ? OR BLOCK? ? OR ELEM-
             ENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? OR BIT OR BITS)(3W)-
             S2:S5
S7      83735   (DIFFERENT OR SEPARATE OR ANOTHER OR OTHER OR RELATED OR N-
             EIGHBOR? OR ADJACENT OR SUBSEQUENT OR SUCCEEDING OR SUCCESSIVE
              OR CONSECUTIVE OR NEXT OR CONTIGUOUS OR BORDERING OR ADJOINI-
             NG OR SECOND??? OR 2ND)(5W)S6
S8      46572   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR SCRAMBL?
S9        655   S8(5N)S7
S10         4   S1(100N)S9
S11   1848919   PART OR PARTS OR PORTION? ? OR FRAGMENT? ? OR SECTION? ? OR
              SEGMENT? ? OR FRACTION? ? OR ASPECT? ?
S12   1660400   BLOCK? ? OR ELEMENT? ? OR ZONE? ? OR REGION? ? OR BYTE? ? -
             OR BIT OR BITS
S13       126   S1(100N)S6(100N)S8
S14        88   S1(50N)S6(50N)S8
S15        22   S14 AND AC=US/PR AND AY=(1970:2000)/PR
S16        22   S14 AND AC=US AND AY=1970:2000
S17        43   S14 AND PY=1970:2000
S18        53   S10 OR S15:S17
S19        53   IDPAT (sorted in duplicate/non-duplicate order)
```

19/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01951853
Secure processor with external memory using block chaining and block re-ordering
Gesicherter Prozessor mit externem Speicher unter Verwendung von Block-Chaining und Wiederherstellung der Blockenreihenfolge
Processeur securise avec memoire externe utilisant le chainage par blocs et resequencement des blocs
PATENT ASSIGNEE:
GENERAL INSTRUMENT CORPORATION, (1403172), 101 Tournament Drive Horsham, , Pennsylvania 19044, (US), (Applicant designated States: all)
INVENTOR:
Candelore, Brant, 10124 Quail Glen Way, Escondido, California 92029, (US)
Sprunk, Eric, 6421 Cayenne Lane, Carlsbad, California 92009, (US)
LEGAL REPRESENTATIVE:
Hoeger, Stellrecht & Partner Patentanwalte (100381), Uhlandstrasse 14 c, 70182 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1571523 A1 050907 (Basic)
APPLICATION (CC, No, Date): EP 2005011051 981006;
PRIORITY (CC, No, Date): US 949111 971010
DESIGNATED STATES: DE; FR; GB; NL
RELATED PARENT NUMBER(S) - PN (AN):
EP 908810 (EP 98118843)
INTERNATIONAL PATENT CLASS (V7): G06F-001/00; G06F-012/14; H04L-009/32; H04L-029/06
ABSTRACT WORD COUNT: 147
NOTE:
Figure number on first page: 6

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200536 1997
SPEC A (English) 200536 17196
Total word count - document A 19193
Total word count - document B 0
Total word count - documents A + B 19193

...SPECIFICATION would actually be data which is never processed.
The external storage device 110 may be **encrypted** such that the **blocks** of program **information** , and authentication information are stored in non-sequential address location in the storage device. It would be preferable to include the high order address bits in **encryption** of the storage device so that any **block** of program **information** may be located anywhere in the memory space. **Substitution tables** (S-tables) can be used to eliminate regularity and add non-linearity in the address **encryption** .
Specifically, the authenticated block chained external storage device is **encrypted** so that the execution of the cryptographic code can be concealed from a pirate who...

...path 113. A pirate may be prevented from learning about the proprietary algorithms being executed. **Encrypting** may therefore prevent a pirate from ascertaining the contents of the storage device, and from systematically attacking the secure circuit 105 through other means with the hardware. **Encryption** of the storage device prevents the pirate from knowing exactly which **encrypted** program information is the likely target for attack. By knowing exactly which program information could...

...with the appropriate byte or block at the right time. Individual strings of sub-fields, **bytes** or **blocks** of **data** from the external storage device are then transferred to the block buffers in a desired...

...deciphering circuits to allow these circuits to descramble the data to function accordingly.
Various block **encryption** algorithms, such as triple DES, may be used. Furthermore, the **scrambling** algorithm may use the same **substitution box** (**S - box**) tables as DES but with fewer rounds. The number of rounds may be selectable forinformation can prevent a pirate from moving otherwise properly **encrypted** and authenticated block chains around in storage device to get the decoder to process program...

19/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

01434552
Methods and apparatus for implementing a cryptography engine
Verfahren und Vorrichtung zur Ausfuhrung einer kryptographischen Funktion
Procede et dispositif de realisation d'une fonction cryptographique
PATENT ASSIGNEE:
Broadcom Corporation, (2064671), 16215 Alton Parkway, Irvine, California 92618, (US), (Applicant designated States: all)
INVENTOR:
Qi, Zheng, 13 Jacklin Circle, Milpitas, California 95035, (US)
Buer, Mark, 1027 E Betsy Lane, Gilbert, Arizona 85296, (US)
LEGAL REPRESENTATIVE:
Jehle, Volker Armin, Dipl.-Ing. (95141), Patentanwalte Bosch, Graf von Stosch, Jehle, Fluggenstrasse 13, 80639 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1215843 A2 020619 (Basic)
EP 1215843 A3 031015
APPLICATION (CC, No, Date): EP 2001309324 011102;
PRIORITY (CC, No, Date): US 255562 P 001213; US 892242 010626
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
ABSTRACT WORD COUNT: 95
NOTE:
Figure number on first page: 5

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200225	797
SPEC A	(English)	200225	6716
Total word count - document A			7513
Total word count - document B			0
Total word count - documents A + B			7513

...SPECIFICATION processing, such as DES and triple DES processing. DES specifies encrypting individual 64-bit data **blocks** . A 64- **bit data block** of unencrypted **data** is provided to the DES engine, combined with a key, and output as a 64- **bit data block** of **encrypted data** . The key used for DES processing is typically a 56-bit number, although the key can be expressed as a 64-bit number. DES describes breaking up a 64- **bit block** of **data** into a right half and a left half, each 32-bits long. As will be...

...performed. In each round, operations on the right half of the data include expansion, permutation, **Sbox** operations, and combination with a round key. A round key can be determined based on...

19/3,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2006 European Patent Office. All rts. reserv.

00907854
CRYPTOGRAPHIC METHOD AND APPARATUS FOR NON-LINEARLY MERGING A DATA BLOCK AND A KEY
KRYPTOGRAPHISCHES VERFAHREN UND EINRICHTUNG ZUM NICHTLINEAREN ZUSAMMENFUGEN EINES DATENBLOCKS UND EINES SCHLUSSELS
PROCEDE ET APPAREIL CRYPTOGRAPHIQUES DE FUSION NON LINEAIRE D'UN BLOC DE DONNEES ET D'UN CODE
PATENT ASSIGNEE:
Koninklijke Philips Electronics N.V., (200769), Groenewoudseweg 1, 5621 BA Eindhoven, (NL), (Proprietor designated states: all)
INVENTOR:
DEN BOER, Huibert, Prof. Holstlaan 6, NL-5656 AA Eindhoven, (NL)
LEGAL REPRESENTATIVE:
Groenendaal, Antonius Wilhelmus Maria et al (59381), INTERNATIONAAL OCTROOIBUREAU B.V., Prof. Holstlaan 6, 5656 AA Eindhoven, (NL)
PATENT (CC, No, Kind, Date): EP 839418 A1 980506 (Basic)
EP 839418 B1 030502
WO 97044935 971127
APPLICATION (CC, No, Date): EP 97919606 970513; WO 97IB544 970513
PRIORITY (CC, No, Date): NL 103159 960520
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200318	1395
CLAIMS B	(German)	200318	1563
CLAIMS B	(French)	200318	1596
SPEC B	(English)	200318	4950
Total word count - document A			0
Total word count - document B			9504
Total word count - documents A + B			9504

...SPECIFICATION to the key, followed by a second processing step of non-linearly processing the result (**S - boxes**). According to the invention, an algorithm is used which non-linearly merges data with a key in one step (i.e. one, sequentially inseparable step). As such, adding the key **bits** to the **data** is an integrated part of the non-linear operation, making the system more immune against...

...in each round both parts of the digital input block are processed, giving a better **encryption** result than for conventional Feistel ciphers, such as DES, where during each round only half...

19/3,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00866163
CONSTRUCTING SYMMETRIC CIPHERS USING THE CAST DESIGN PROCEDURE
ENTWURF SYMMETRISCHER VERSCHLUSSELUNGSVERFAHREN NACH DEM CAST-VERFAHREN
CREATION D'ALGORITHMES CRYPTOGRAPHIQUES PAR LA PROCEDURE DE CONCEPTION CAST
PATENT ASSIGNEE:
ENTRUST TECHNOLOGIES LTD., (2538870), 750 Heron Road, Tower E, Ottawa, Ontario K2G 5J9, (CA), (Proprietor designated states: all)
INVENTOR:
ADAMS, Carlisle, Michael, 1182 Soderlind Street, Ottawa, Ontario K2C 3B4, (CA)
WIENER, Michael, James, 20 Hennepin Street, Nepean, Ontario K2J 3Z4, (CA)
LOCKHART, Roland, Thomas, 27 Liston Crescent, Kanata, Ontario K2L 2W3, (CA)

LEGAL REPRESENTATIVE:
  Newstead, Michael John et al (34355), Page Hargrave Southgate,
    Whitefriars Lewins Mead, Bristol BS1 2NT, (GB)
PATENT (CC, No, Kind, Date): EP 953244 A1 991103 (Basic)
                              EP 953244 B1 021023
                              WO 97022192 970619
APPLICATION (CC, No, Date):   EP 96938884 961127; WO 96CA782 961127
PRIORITY (CC, No, Date): CA 2164768 951208
DESIGNATED STATES: CH; DE; DK; ES; FI; FR; GB; IT; LI; NL
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
NOTE:
  No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language   Update   Word Count
      CLAIMS B (English) 200243   993
      CLAIMS B   (German) 200243   975
      CLAIMS B   (French) 200243   1381
      SPEC B   (English) 200243   5431
Total word count - document A   0
Total word count - document B   8780
Total word count - documents A + B   8780

...SPECIFICATION it uses three variations of the round function itself
  throughout the cipher. Finally, the 8x32 **s - boxes** used in the round
  function each have a minimum nonlinearity of 74 and a maximum...

...table.
    This example cipher appears to have cryptographic strength in
  accordance with its keysize (80 **bits**) and has very **good** **encryption**
  / decryption performance: over 1 MByte/sec on a 486-DX2 66MHz PC, and
  over 2...

...CLAIMS the second masking key, and the half data block being operated
      upon.
  12. The data **encryption** method of cryptographically transforming
      plaintext into ciphertext in data blocks of predetermined bitlength
      according to...

...are fully specified for all implementations of the method and is
      independent of any key **bits** or **data** **bits** .
  13. The **data** **encryption** method of cryptographically transforming
      plaintext into ciphertext in data blocks of predetermined bitlength
      according to...

...to combine the half data block with the first masking key and to combine
      the **s - box** outputs which result from the processing of the **second**
       modified half data **block** .
  14. The **data** **encryption** method of cryptographically transforming
      plaintext into ciphertext in data blocks of predetermined bitlength
      according to...

 19/3,K/10   (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00697290
SYSTEM AND APPARATUS FOR BLOCKWISE ENCRYPTION/DECRYPTION OF DATA
SYSTEM UND ANORDNUNG ZUM BLOCKWEISEN VERSCHLUSSELN/ENTSCHLUSSELN VON DATEN
SYSTEME ET APPAREIL POUR LE CRYPTAGE/DECRYPTAGE EN BLOCS DE DONNEES
PATENT ASSIGNEE:
  IRDETO B.V., (1944790), Jupiterstraat 42, 2132 HD Hoofddorp, (NL),
    (applicant designated states:
    AT;BE;CH;DE;DK;ES;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:
KUHN, Gideon Jacobus, 108 Farnham Road, Lynnwood Manor, Pretoria 0081, (ZA)
DAVIES, Donald Watts, 15 Hawkewood Road, Sunbury-on-Thames, Middlesex TW16 6HL, (GB)
RIX, Simon, Paul Ashley, 51IXia Road, Primrose Hill Genniston, Transvaal, (ZA)
LEGAL REPRESENTATIVE:
de Vries, Johannes Hendrik Fokke (46334), De Vries & Metman, Overschiestraat 184 N, 1062 XK Amsterdam, (NL)
PATENT (CC, No, Kind, Date): EP 723726 A1 960731 (Basic)
EP 723726 B1 990224
WO 9510906 950420
APPLICATION (CC, No, Date): EP 95901624 941007; WO 94NL245 941007
PRIORITY (CC, No, Date): NL 931784 931014
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS (V7): H04L-009/06;
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9907	651
CLAIMS B	(German)	9907	587
CLAIMS B	(French)	9907	682
SPEC B	(English)	9907	1784
Total word count - document A			0
Total word count - document B			3704
Total word count - documents A + B			3704

...SPECIFICATION having 8 bits, which look-up table is also referred to as substitution module or S -box. The output of the S-box 12 is applied to the XOR element ahead...
...is indicated by R1, R2 ... R7. Of course it is also possible to repeat the **encryption** process a higher or lower number of times.
In contrast to known **encryption** algorithms, like the DES algorithm, a single relatively large S- **box** is used in the described **encryption** device instead of a plurality of small **S - box** elements. The use of one large **S - box** shows the advantage that a very strong non-linearity is introduced in one step. The...

...is directly combined with a byte of the key and the operation provided by the **S - box** provides a strong non-linearity introduced in memory element 7 and after permutation through the...

...5. As the byte modified in a non-linear manner at the output of the **S - box**, 12 is introduced into the shift register 8 at two locations, a rapid diffusion of this non-linearity is obtained. Thereby a better **encryption** is obtained then would be possible by means of a plurality of small **S - box** elements. The use of the XOR element between the memory elements 2 and 3 of...

...of a data block with the complement of the key and the complement of the **encrypted** data block.
As shown in Fig. 3, decryption is obtained by the reversed operation. It...

19/3,K/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00450088
ENCRYPTION METHOD

VERSCHLUSSELUNGSMETHODE
METHODE DE CHIFFREMENT

PATENT ASSIGNEE:
CRYPTECH, INC., (1343120), 34, Severn Parkway, Jamestown, NY 14701, (US),
(applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
WOOD, Michael, C., 147 Prather Avenue, Jamestown, NY 14701, (US)
LEGAL REPRESENTATIVE:
Land, Addick Adrianus Gosling et al (59332), Arnold & Siedsma, Advocaten
en Octrooigemachtigden, Sweelinckplein 1, 2517 GK Den Haag, (NL)
PATENT (CC, No, Kind, Date): EP 489742 A1 920617 (Basic)
EP 489742 A1 930317
EP 489742 B1 971119
WO 9103113 910307
APPLICATION (CC, No, Date): EP 90911008 900314; WO 90US1391 900314
PRIORITY (CC, No, Date): US 395448 890817
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04L-009/06;
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9711W2	1540
CLAIMS B	(German)	9711W2	1499
CLAIMS B	(French)	9711W2	1646
SPEC B	(English)	9711W2	14641
Total word count - document A			0
Total word count - document B			19326
Total word count - documents A + B			19326

...SPECIFICATION is eight characters in length. A good example of a modern system is the Data **Encryption** Standard ("DES") which was developed by IBM in the early 1970's and which was adopted by the United States Bureau of Standards as the standard **encryption** system for business and non-military government use. Patents directed to the DES include U.S. Patents Nos. 3,958,081 and 3,962,539. The Data **Encryption** Standard is a block type of cipher in which a portion or **block** of the **data** to be **encrypted** is permutated with a prearranged permutation table, modified with a key, and then substituted with a predetermined **substitution table** . This process is repeated numerous times in what are referred to as rounds. Permutation is...

...is a common cryptographic function in which the positions of letters in a message are **scrambled** in accordance with a predetermined set of directions.

Other modern **encryption** systems have attempted to simulate the key generation process of a one time pad by...first block of plaintext is selected. Although FIG. 1 is shown in connection with the **encipherment** of blocks of plaintext, the same steps would also be followed for decrypting selected blocks of ciphertext. Control then passes to reference 16 where the selected block of plaintext is **encrypted** in accordance with the cryptographic system of the present invention. If there is more plaintext left to be **encrypted** , as determined by query 18, the next block of plaintext is selected at reference 20 and the next block is **encrypted** . If there is no more plaintext, then the system stops operation at reference 22.

The...

...tables in memory is shown in more detail in FIG. 2. A permutation table, an **S - box** table and an enclave table are initially loaded into the system's memory at reference...

...entries which dictate in a particular fashion how the position of the bytes in the **block** of **data** undergoing **encryption** will be **scrambled** , or will be descrambled for decryption. This is a commonly used

cryptographic technique. The **S - box** table is an arrangement for a plurality of substitution entries which dictate, as directed by...

...changed to another value. While this could be included in the form of a standard **substitution table** , the **S - box** table arrangement is more efficient computationally and is well-known in the field of cryptography ...The position of the eight bit bytes at the top of FIG. 4 will be **scrambled** as directed by the various arrows to the new position shown at the bottom of FIG. 4. Working from the top to the bottom gives an **encryption** of the data. To decrypt the data, the positioning is rearranged from the bottom to...not be explained in further detail in this application. Likewise, a typical entry in the **substitution table** is shown in FIG. 5. If a particular plaintext value appears in any of the **bytes** of the **data** undergoing transformation, then the **substitution table** used will direct that the plaintext value be substituted by a new value. For instance...

...5, it will be substituted by the new value of S1)). Working backwards through the **substitution table** , the **encrypted** data can then be decrypted to recapture the original plaintext values. Once again, this is ...

...in FIGS. 4 and 5 are only representative of the many possibilities of permutation and **substitution table** entries and that many other entries would be included in the tables used in the...bC. This is represented by the series of querys at element 180 associated with each **byte** of the **data** undergoing transformation at element 170. If C is equal to the byte number, then that byte is not combined with the corresponding key **byte** . The **block** of **data** after it has undergone a round of the variable key addition is shown as element 182 in FIG. 10.
The variable substitution for the **encryption** process shown in FIG. 8 is shown in more detail in FIG. 11. Similar to...

...substitution. Otherwise, the steps followed in each are the same. In the substitution process, the **S - Box** chosen Z is determined by **byte** C in the **data** undergoing transformation and Mask4,R)). This is shown in FIG. 11 where Z is equated...block in element 250 is then substituted in accordance with the protocol of the chosen **S '- Box** except for byte bC. The result of the inverse variable substitution is a ten **byte data** block B1 through B10 at element 260. The arrangement by which byte bC is not substituted is shown by a series of querys 258 associated with each **byte** of the **data** undergoing decryption in element 250. For example, in thefirst round of decryption, where R is ten, b10 is both used to select the **S '- Box** used for the inverse substitution and is also unchanged during the inverse substitution. Since the...

...byte remained unchanged during the final variable substitution carried out on the data during the **encryption** process shown in FIG. 8, it is possible to recreate and work backwards through the **encryption** process through the ciphertext data. The same is true for the inverse variable key addition...

...of the steps taken in the variable enclave for encryption shown in FIG. 6. The **block** of **data** undergoing decryption at element 270 is split into a left half-block 272 and a...at element 330 as bytes B1 through B10. Since during the encryption process all ten **bytes** of the **data** undergoing encryption were used to select a permutation table for the transformation, this rendered it possible to decrypt the same data by once again adding together all ten **bytes** of the ciphertext **data** to determine which permutation table should be used. This is possible since the permutation operation merely rearranged the order of the values. The information used in the **encryption** stage can be extracted by once again summing together the values in the data.

EXAMPLE

An example of the **encryption** of a ten **byte** **block** of plaintext **data** using the embodiment of the **encryption** system of the present invention discussed above will now be shown in detail. The system must be initialized with a permutation table, a **substitution** **table** and an enclave table. Tables used in this example, and created in accordance with the...generated from the initial key (which is not included in either table), data can be **encrypted** using additionally the permutation, enclave and **substitution** **tables** in Tables I, IIA and IIB, and III below. A particular **block** of plaintext **data** will be **encrypted** under the system of the present invention and for ten rounds of **encryption** .

ROUND 1
BLOCK = 104 101 108 108 111 32 116 104 101 114
(a) Variable...

19/3,K/15 (Item 15 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01217421
Data encrypton apparatus and method
Verfahren und Vorrichtung zur Datenverschlusselung
Procede et appareil de cryptage de donnees
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Yokota, Kaoru, 3-9-202, Shinnozukacho, Ashiya-shi, Hyogo-ken 659-0016, (JP)
Ohmori, Motoji, 1-9-3-402, Nasuzukuri, Hirakata-shi, Osaka-fu 573-0071, (JP)
Miyaji, Atsuko, 1-50-D-34, Asahidai, Tatsunokuchi-cho, Noumi-gun, Ishikawa-ken 923-1211, (JP)
LEGAL REPRESENTATIVE:
Crawford, Andrew Birkby et al (29761), A.A. Thornton & Co. 235 High Holborn, London WC1V 7LE, (GB)
PATENT (CC, No, Kind, Date): EP 1056240 A1 001129 (Basic)
EP 1056240 B1 030319
APPLICATION (CC, No, Date): EP 99310637 991230;
PRIORITY (CC, No, Date): JP 99146079 990526
DESIGNATED STATES: DE; FR; GB; IT
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
ABSTRACT WORD COUNT: 81
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200048	1098
CLAIMS B	(English)	200312	1267
CLAIMS B	(German)	200312	1070
CLAIMS B	(French)	200312	1606
SPEC A	(English)	200048	8951
SPEC B	(English)	200312	9066
Total word count - document A			10051
Total word count - document B			13009
Total word count - documents A + B			23060

...SPECIFICATION 3002 in the data converting unit 300 (301) performs an exclusive-OR operation for corresponding **bits** in input **data** X and two shift-rotation results of the input data X that are data Rot7(X) and data

Rot1(X). Accordingly, the change in a single **bit** in the input **data** X affects not only the bit itself but another two **bits** . Besides, output **data** of the data substituting unit 3002 is further processed nonlinearly in the **substitution table** data storing unit 3003, as a result of which many more bits will end up being affected.

Thus, the data converting unit 300 (301), i.e. the data **encryption** apparatus 10, in this embodiment produces a high bit avalanche effect unlike the conventional techniques...

...number (no less than 3) of different shift-rotations (including a shift-rotation by 0 **bit**) on input **data** and takes an exclusive-OR for corresponding bits in the input data and the shift...

...SPECIFICATION avalanche effect referred to here is the observed property of a cipher on how many **bits** in the output **data** change as a result of the change of a single **bit** in the input **data** .

US-A-5,724,428 discloses a simple **encryption** and description device in which the underlying algorithm is a fast block cipher that makes...

...a linear transformation; and a final permutation. Each round uses only a single replicated S- **box** .

SUMMARY OF THE INVENTION

In view of the above problems, the present invention aims to...

...ability and that produces a sufficient bit avalanche effect.

The present invention provides a data **encryption** apparatus provided with a data converting device for converting n- **bit** input **data** to n- **bit** output **data** , the **data** converting device comprising:

shift-rotating means for generating k sets-of data by shirt-rotating the n- **bit** input **data** ; and

data combining means for combining together the k sets of data to generate the output data, characterised in that the shift-rotating means shift rotates the n- **bit** input **data** respectively by S1 bits, S2 bits, ..., and Sk bits, S1, S2, ..., and Sk being nonnegative...3002 in the data converting unit 300 (301) performs an exclusive-OR operation for corresponding **bits** in input **data** X and two shift-rotation results of the input data X that are data Rot7(X) and data Rot1(X). Accordingly, the change in a single **bit** in the input **data** X affects not only the bit itself but another two **bits** . Besides, output **data** of the data substituting unit 3002 is further processed nonlinearly in the **substitution table** data storing unit 3003, as a result of which many more bits will end up being affected.

Thus, the data converting unit 300 (301), i.e. the data **encryption** apparatus 10, in this embodiment produces a high bit avalanche effect unlike the conventional techniques...number (no less than 3) of different shift-rotations (including a shift-rotation by 0 **bit**) on input **data** and takes an exclusive-OR for corresponding bits in the input data and the shift...

19/3,K/16 (Item 16 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01210193

A dynamic validation system

Dynamisches System zur Gultigkeitserklarung

Systeme dynamique de validation

PATENT ASSIGNEE:

Sientescom Developments Limited, (2776560), Wilton Place, Dublin 2, (IE), (Applicant designated States: all)

INVENTOR:

Roche, Patrick John, 19 The Circle, Broadale, Maryborough Hill, Douglas, County Cork, (IE)

Walshe, John, Nadrid, Coachford, County Cork, (IE)
Fitzpatrick, Patrick, 34 Woodbrook Avenue, Bishopstown, Cork, (IE)
Murnane, Liam, 106 The Drive, Broadale, Maryborough Hill, Douglas, County Cork, (IE)
LEGAL REPRESENTATIVE:
O'Connor, Donal Henry (72401), c/o Cruickshank & Co., 1 Holles Street, Dublin 2, (IE)
PATENT (CC, No, Kind, Date): EP 1050991 A1 001108 (Basic)
APPLICATION (CC, No, Date): EP 99650038 990427;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/00
ABSTRACT WORD COUNT: 170
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200045	716
SPEC A	(English)	200045	7568
Total word count - document A			8284
Total word count - document B			0
Total word count - documents A + B			8284

...SPECIFICATION between T and S by an attacker during the key exchange.
As mentioned above, the **encryption** /decryption algorithm for this system is the DES algorithm with **S - box** which is a standard hardware algorithm to **encrypt** data. DES is widely used by banks and financial institutions to protect financial transactions which...

...for hardware implementation enabling real-time data to be securely exchanged between users.
The Data **Encryption** Standard (DES) is a **block** cipher, operating on **data** in 64 bit blocks. A 64 bit block of plaintext is transformed into a 64...

...is a symmetric algorithm, this means that the same algorithm and key are used for **encryption** and decryption. The key is 56 bits in length and any 56-bit value can...

...operation of the S-boxes. There are eight S-boxes, each of which accepts 6 **bits** of the **data** as input and gives a 4-bit output, thus reducing the size of the data...input specifies the row and column in which the output appears. The composition of the **S boxes** can vary. The purpose of this feature of the **S - box** is to increase the security of the **encryption** of data.
Finally, the 32- **bit data** is permuted again. This is a simple permutation, mapping each one of the 32 input...

...The decryption process of transforming ciphertext into plaintext uses the same function f as the **encryption** process. The only difference is that the keys must be used in the reverse order. Thus, if the keys for **encryption** are K1)), K2)), K3)), ..., K16)), then the keys for decryption are K16)), K15)), K14)), ..., K1...

19/3,K/17 (Item 17 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01161013
COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM

GEGENMASSNAHMENVERFAHREN IN EINEM ELEKTRONISCHEN BAUELEMENT. DAS EIN ALGORITHMUS MIT EINEM PRIVATEN SCLHUSSEL VERWENDET
PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE
PATENT ASSIGNEE:
GEMPLUS, (1705263), Avenue du Pic de Bertagne, Parc d'Activites de Gemenos, 13881 Gemenos Cedex, (FR), (Proprietor designated states: all)
INVENTOR:
CLAVIER, Christophe, 5, rue de la Republique, F-13420 Gemenos, (FR)
BENOIT, Olivier, La Treille d'Azur, Bat. D, Avenue du 19 Mars 1962, F-13400 Aubagne, (FR)
PATENT (CC, No, Kind, Date): EP 1119940 A1 010801 (Basic)
EP 1119940 B1 050921
WO 2000024156 000427
APPLICATION (CC, No, Date): EP 99942981 990915; WO 99FR2199 990915
PRIORITY (CC, No, Date): FR 9812990 981016
DESIGNATED STATES: DE; ES; FR; GB; IT
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): French; French; French
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200538	600
CLAIMS B	(German)	200538	526
CLAIMS B	(French)	200538	587
SPEC B	(French)	200538	6802
Total word count - document A			0
Total word count - document B			8515
Total word count - documents A + B			8515

...SPECIFICATION Avec une attaque DPA, on est capable de reconstituer au moins 48 bits des 56 **bits** utiles.
Trois **documents** se rapprochant de l'invention peuvent etre cites.
Le premier document de Yi X. dont le titre anglais est <<A method for obtaining cryptographically strong 8X8 **S - BOXES** >>, document publie a la conference sur les telecommunications a Phoenix, Arizona, Etats-Unis d'Amerique...

...une bonne propriete contre l'attaque differentielle permettant par l'utilisation de tables de constantes **SBOX** d'accroitre la securite des systemes cryptographiques.
Le second document de Miyaguchi S. dont le titre anglais est <<Secret key ciphers that change the **encipherment** algorithm under the control of the key>>, document publie dans la revue << NTT REVIEW >>, vol...

...permutations entre les tables de constantes elementaires S1 a S8 d'une table de constantes **S - BOX** . La methode est resistante contre les attaques qui calculent la cle en utilisant des paires...

19/3,K/18 (Item 18 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01161012
COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM
GEGENMASSNAHMENVORRICHTUNG IN EINEM ELKTRONISCHEN BAUTEIL UM EINEN KRYPTO-ALGORITHMUS MIT GEHEIMSCHLUSSEL DURCH ZU FUHREN
PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE
PATENT ASSIGNEE:
GEMPLUS, (1705263), Avenue du Pic de Bertagne, Parc d'Activites de Gemenos, 13881 Gemenos Cedex, (FR), (Proprietor designated states: all)

INVENTOR:
  CLAVIER, Christophe, 5 rue de la Republique, F-13420 Gemenos, (FR)
  BENOIT, Olivier, La Treille d'Azur,Batiment D. avenue 19 Mars 1962, F-13400 Aubagne, (FR)
PATENT (CC, No, Kind, Date): EP 1119939 A1 010801 (Basic)
EP 1119939 B1 051130
WO 2000024155 000427
APPLICATION (CC, No, Date): EP 99942957 990913; WO 99FR2172 990913
PRIORITY (CC, No, Date): FR 9812989 981016
DESIGNATED STATES: DE; ES; FR; GB; IT
INTERNATIONAL PATENT CLASS (V7): H04L-009/06
NOTE:
  No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): French; French; French
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200548	864
CLAIMS B	(German)	200548	781
CLAIMS B	(French)	200548	872
SPEC B	(French)	200548	6193
Total word count - document A			0
Total word count - document B			8710
Total word count - documents A + B			8710

...SPECIFICATION de Yi X. dont le titre anglais est <<A method for obtaining cryptographically strong 8X8 **S - BOXES** >>, document publie a la conference sur les telecommunications a Phoenix, Arizona, Etats-Unis d'Amerique...

...une bonne propriete contre l'attaque differentielle permettant par l'utilisation de tables de constantes **SBOX** d'accroitre la securite des systemes cryptographiques.
. Le second document de Miyaguchi S. dont le titre anglais est <<Secret key ciphers that change the **encipherment** algorithm under the control of the key>>, document publie dans la revue << NTT REVIEW >>, vol...

...permutation entre les tables de constantes elementaires S1 a S8 d'une table de constantes **S - BOX** . La methode est resistante contre les attaques qui calculent la cle en utilisant des paires...

19/3,K/19 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01160614
Information processing equipment
Datenverarbeitungsanlage
Dispositif de traitement de donnees
PATENT ASSIGNEE:
  Hitachi, Ltd., (204151), 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Proprietor designated states: all)
INVENTOR:
  Oki, Masaru, c/o Hitachi, Ltd., Intellectual Pro., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
  Fukuzawa, Yasuko, c/o Hitachi, Ltd., Intell. Prop., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
  Okuhara, Susumu c/o Hitachi, Ltd., Intell. Pro., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
  Kaminaga, Masahiro c/o Hitachi, Ltd., Intell. Pro., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
  Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1011081 A1 000621 (Basic)

EP 1011081 B1 030319
APPLICATION (CC, No, Date): EP 99124934 991214;
PRIORITY (CC, No, Date): JP 98354156 981214
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G07F-007/10; G06K-019/073
ABSTRACT WORD COUNT: 78
NOTE:
Figure number on first page: 4

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200025	2129
CLAIMS B	(English)	200312	1738
CLAIMS B	(German)	200312	1535
CLAIMS B	(French)	200312	2060
SPEC A	(English)	200025	9497
SPEC B	(English)	200312	9513
Total word count - document A			11629
Total word count - document B			14846
Total word count - documents A + B			26475

...SPECIFICATION the exclusive logical OR at 1003, to acquire the row and column numbers of an **S box** table and generate 4- **bit data** . The **contents** of the **S box** table change with the position of each 6-bit set. The P permutation process exchanges...

...generated by using a random number generator or a pseudo random number each time an **encryption** (or decryption) process of DES is performed (1102). Different disturbance data is therefore used for...

...SPECIFICATION the exclusive logical OR at 1003, to acquire the row and column numbers of an **S box** table and generate 4- **bit data** . The **contents** of the **S box** table change with the position of each 6-bit set. The P permutation process exchanges...

...generated by using a random number generator or a pseudo random number each time an **encryption** (or decryption) process of DES is performed (1102). Different disturbance data is therefore used for...

19/3,K/20 (Item 20 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01155709
Information processing equipment and IC card
Datenverarbeitungsanlage und -chipkarte
Dispositif et carte a puce pour le traitement de donnees
PATENT ASSIGNEE:
Hitachi, Ltd., (204151), 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Oki, Masaru, c/o HITACHI, Ltd., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
Fukuzawa, Yasuko, c/o HITACHI, Ltd., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
Okuhara, Susumu, c/o HITACHI, Ltd., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
Kaminaga, Masahiro, c/o HITACHI, Ltd., New Marunouchi Bldg., 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1006492 A1 000607 (Basic)

APPLICATION (CC, No, Date): EP 99123518 991125;
PRIORITY (CC, No, Date): JP 98338779 981130
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G07F-007/10; G06F-001/00; G06K-019/073
ABSTRACT WORD COUNT: 101
NOTE:
Figure number on first page: 1 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200023	1618
SPEC A	(English)	200023	10277
Total word count - document A			11895
Total word count - document B			0
Total word count - documents A + B			11895

...SPECIFICATION execution order of these processes is reversed for a routine (1501) to process the inverted **bit** S box **data** at first. Since the P permutation exchanges the bit positions, the bit inverted P permutation...

...relation to the normal P permutation process data as the process result of the normal **S box** process data.
Examples of the f function processes (402 to 405) have been described above...

...of data processes is randomized, a dummy process is added, and the normal data and **bit** inverted **data** are used. It is therefore possible to make it difficult to presume the dependency of...

...a cryptographic algorithm utilizing a difficulty in prime factoring. Since different keys are used for **enciphering** and deciphering, this algorithm is called an anti-symmetric algorithm. For both the enciphering and...